User Manual

BDG561AM
WiFi HSPA VPN Router

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

Table of Contents

Copyright ……..2

FCC Interference Statement ……2

CHAPTER 1 INTRODUCTION 4

1.1 Package List.... 4

1.2 Hardware Installation 5

CHAPTER 2 GETTING START....10

2.1 Easy Setup by Windows Utility 10

CHAPTER 3 MAKING CONFIGURATION 18

3.1 Web Wizard 18

3.2 Advanced Setting 23

3.2.1 Basic Setting.... 23

3.2.2 Forwarding Rules 38

3.2.3 Security Setting 41

3.2.4 Advanced Settings 62

3.2.5 SMS.... 70

3.2.6 Tool Box.... 72

CHAPTER 4 TROUBLESHOOTING....77

APPENDIX A SPEC SUMMARY TABLE....81

APPENDIX B LICENSING INFORMATION 82

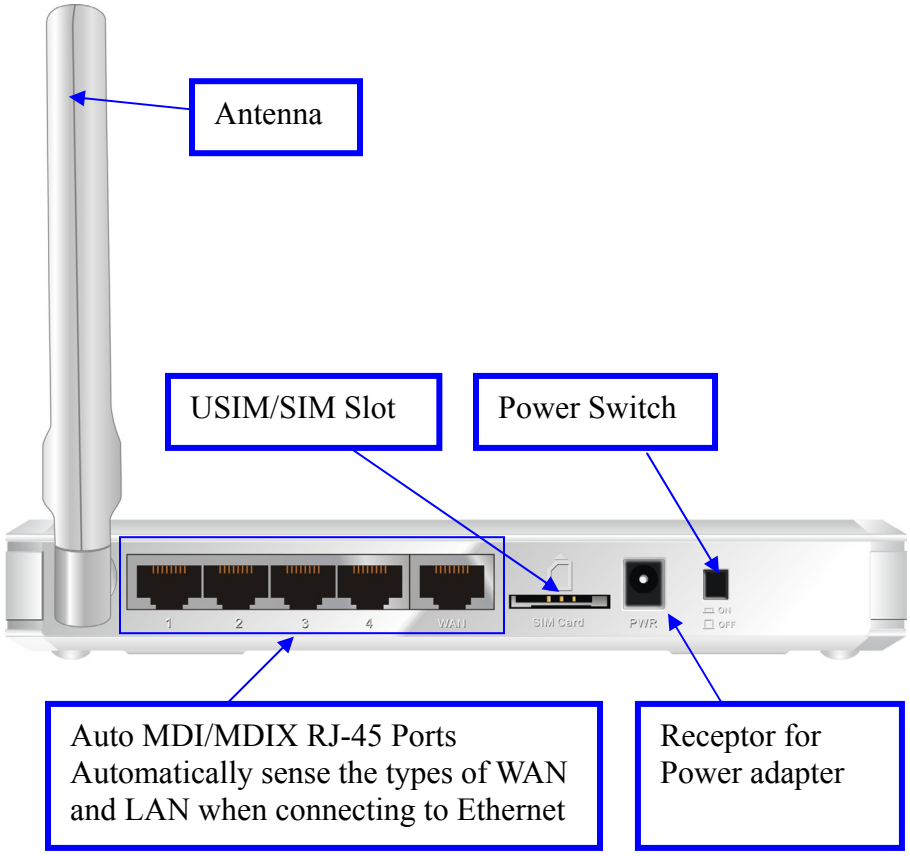
Chapter 1 Introduction

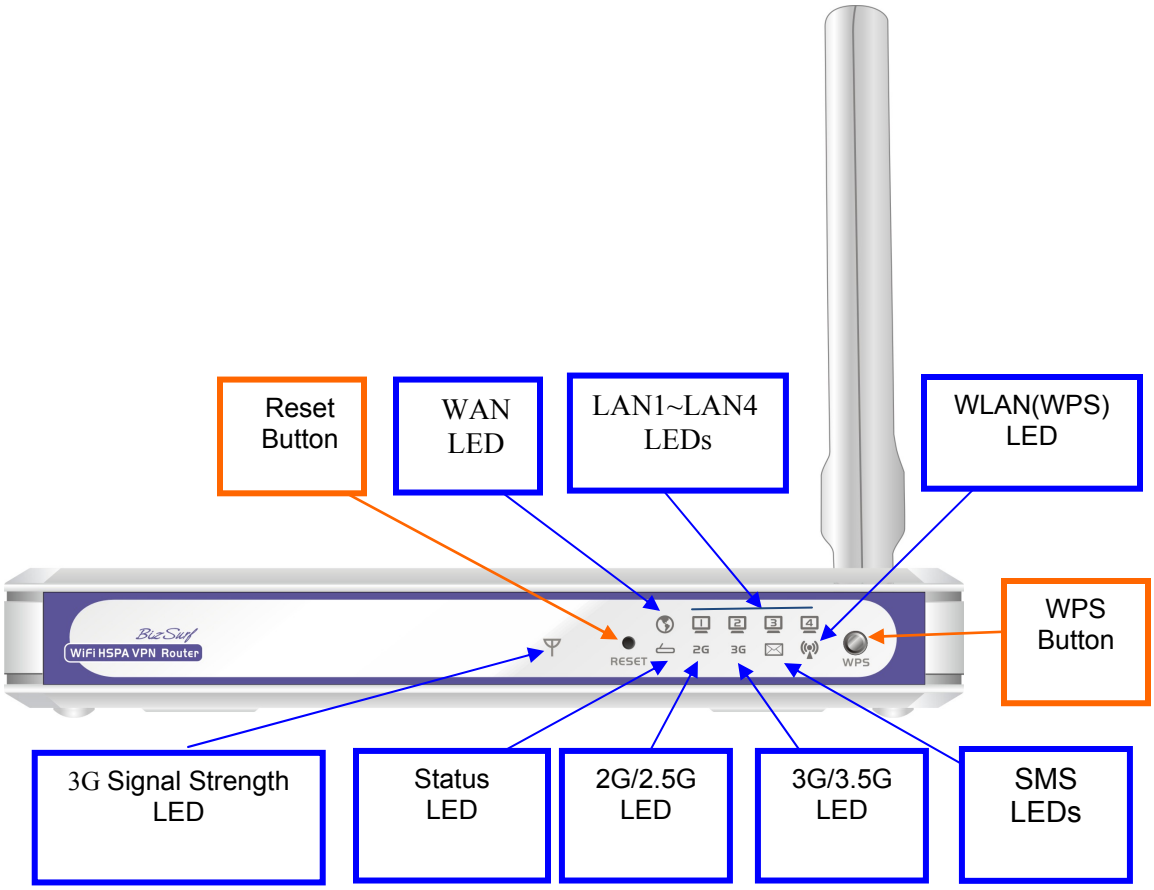
Congratulations on your purchase of this outstanding **BDG561AM**, 802.11n Wireless HSPA VPN Router. The device is a WiFi-supported HSPA router with built-in HSUPA embedded module and supporting IPSec VPN. It supports NAT, routing, firewall, VPN pass-through, auto-3G-dial-up backup connection, DHCP server, and so on. And is easy to configure and operate even for non-technical users. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

1.1 Package List

items	Description	Contents	Quantity
1	WiFi HSPA VPN Router		1
2	Power adapter 12V/1A		1
3	CD Manual		1

1.2 Hardware Installation





LED indicators

	LED status	Description
Status	Green in flash	Device status is working.
3G Signal Strength LED	Red in flash	Disconnected. No SIM card / signal or unverified PIN code
	Amber in flash	Connecting.
	Red	Connected. Signal strength in level one (weak)
	Red in quick flash	Roaming alert, and 3G signal is weak
	Amber	Connected. Signal strength in level two or three (middle)
	Amber in quick flash	Roaming alert, and 3G signal is middle
	Green	Connected. Signal strength in level four or five (strong)

	Green in quick flash	Roaming alert, and 3G signal is strong
2G/2.5G LED	Green	EDGE or GPRS connection is established
	Green in flash	Data packet transferred via 2G/2.5G
3G/3.5G LED	Green	UMTS/HSDPA/HSUPA connection is established
	Green in flash	Data packet transferred via 3G/3.5G
SMS LED	Green	SMS storage is full
	Green in flash	There is any unread SMS in the storage
WAN LED	Green	RJ45 cable is plugged
	Green in flash	Data access
LAN LED	Green	RJ45 cable is plugged
	Green in flash	Data access
WiFi LED	Green	WLAN is on
	Green in flash	Data access
	Green in fast flash	Device is in WPS PBC mode

How to operate

Step 1. Attach the antenna.
1.1. Remove the antenna from its plastic wrapper.
1.2. Screw the antenna in a clockwise direction to the back panel of the unit.
1.3. Once secured, position the antenna upward at its connecting joint. This will ensure optimal reception.
1.4. And rip the “USIM/SIM & PWR” sign label from “Pull” tag.

1. Turn off the Power Switch first.
2. DO NOT connect 802.11n Wireless HSPA Router to power before performing the installation steps below.

Step 2. Insert SIM/USIM to IAD.

NOTE:
2.1. The 802.11n Wireless HSPA Router builds in a HSUPA 3G modem card. Please refer to your service provider for detailed feature information.
2.2. A 3G SIM/USIM Card with data services is MUST.

Step 3. Insert the Ethernet cable into LAN Port:
Insert the Ethernet patch cable into LAN port on the back panel of the 802.11n Wireless HSPA Router, and an available Ethernet port on the network adapter in the computer you will use to configure the unit.

Step 4. Insert the Ethernet patch cable into Wired WAN port:
Insert the Ethernet patch cable into Wired WAN port on the back panel of the 802.11n Wireless HSPA Router.

NOTE: The step does not need if you select the 3G Wireless WAN.

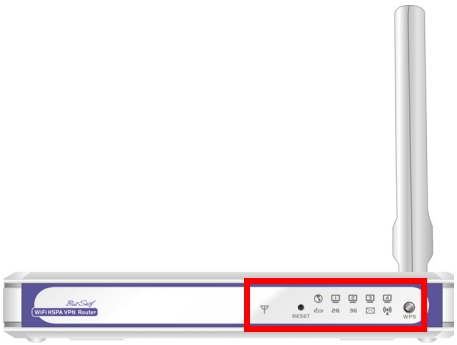
Step 5. Power on the Router:
5.1. Connect the power adapter to the receptor on the back panel of your 802.11n Wireless HSPA Router.
5.2. Then plug the other end of the power adapter into a wall outlet or power strip.
5.3. Turn on the Power Switch.

Step 6. Complete the setup.

6.1. All LEDs will transient illumination to indicate power has been applied.

6.2. And then LEDs will flash ON and OFF as the 802.11n Wireless HSPA Router performs initialization and Internet connection processes. This will take a few minutes.

6.3. When complete, the Status LED will flash.



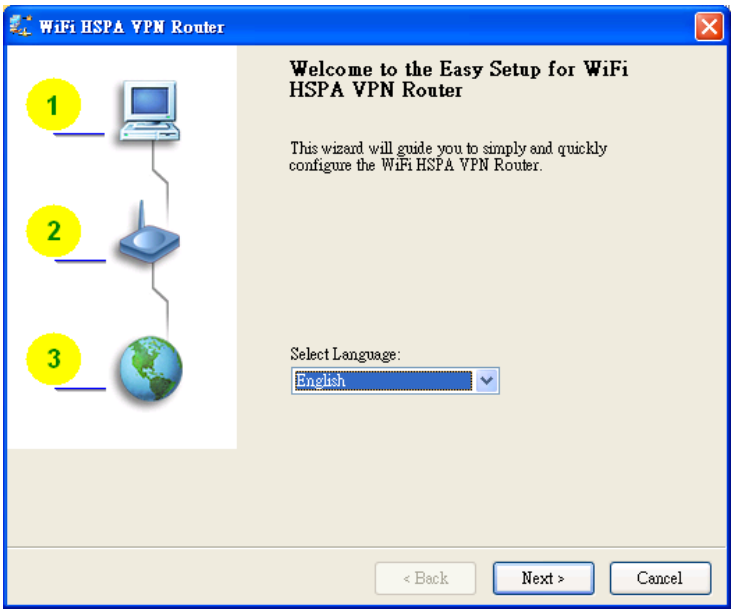
Chapter 2 Getting start

Insert the CD into CD reader on your PC. The program, AutoRun, will be executed automatically. And then you can click the Easy setup Icon for this utility.
Configure the settings by the following steps.

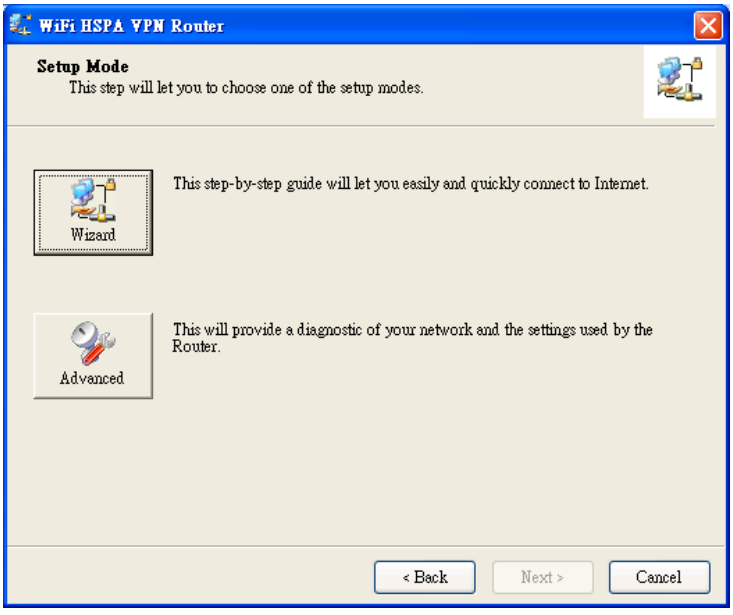
2.1 Easy Setup by Windows Utility

You can also use the Easy Setup Utility to configure it

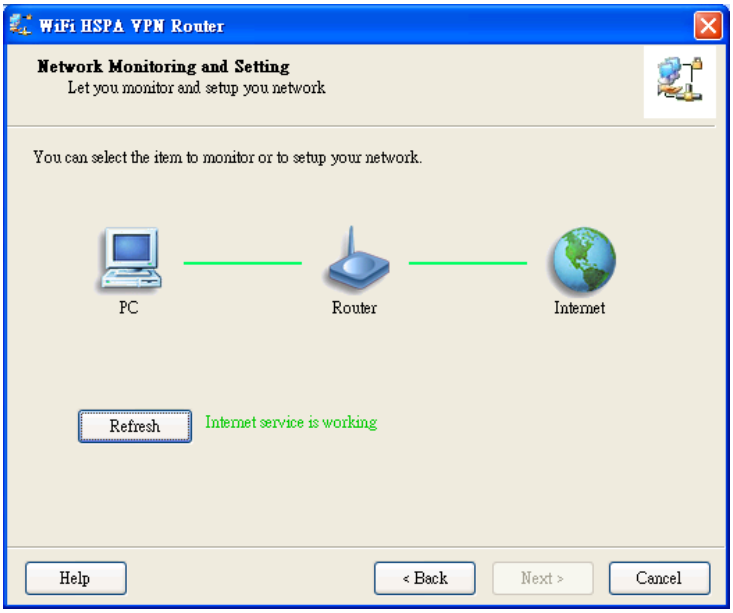
Step 1. Select your language.
Select Language then click “Next” for continues.


WiFi HSPA VPN Router
Welcome to the Easy Setup for WiFi HSPA VPN Router
This wizard will guide you to simply and quickly configure the WiFi HSPA VPN Router.
Select Language:
English
< Back
Next >
Cancel

Step 2. Setup mode
You can select Wizard mode to run the setup step-by-step or run advanced mode to diagnose the network settings of the router.


WiFi HSPA VPN Router
Setup Mode
This step will let you to choose one of the setup modes.
Wizard
This step-by-step guide will let you easily and quickly connect to Internet.
Advanced
This will provide a diagnostic of your network and the settings used by the Router.
< Back
Next >
Cancel

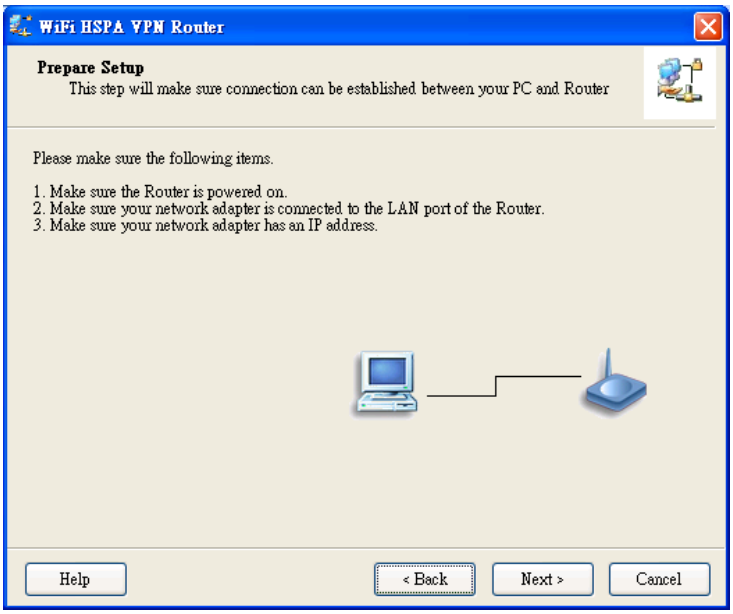
Step 3. Advanced mode Setup.
Check the PC, Router or Internet icons for the Status of PC, Router or Internet.



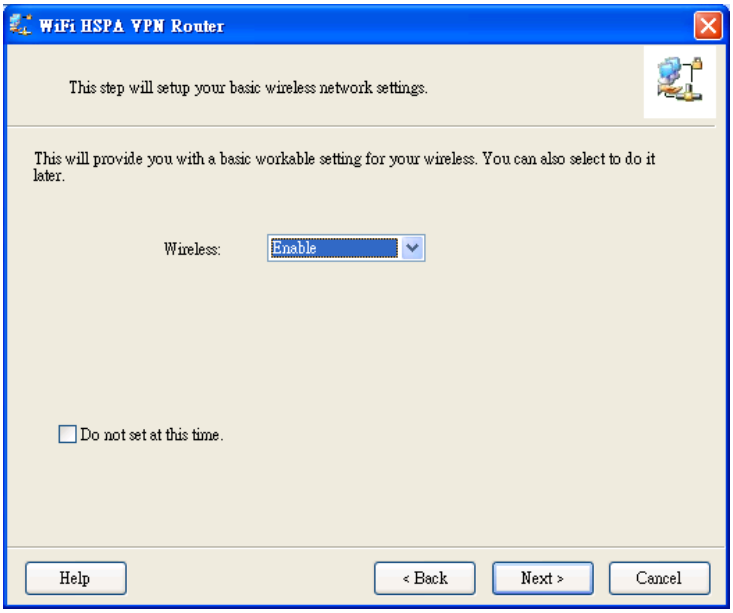
Step 4. Wizard mode-Prepare Setup

1. Make sure the router is powered on.
2. Make sure your network adapter is connected to the LAN port of the router
3. Make sure your network adapter has an IP address.

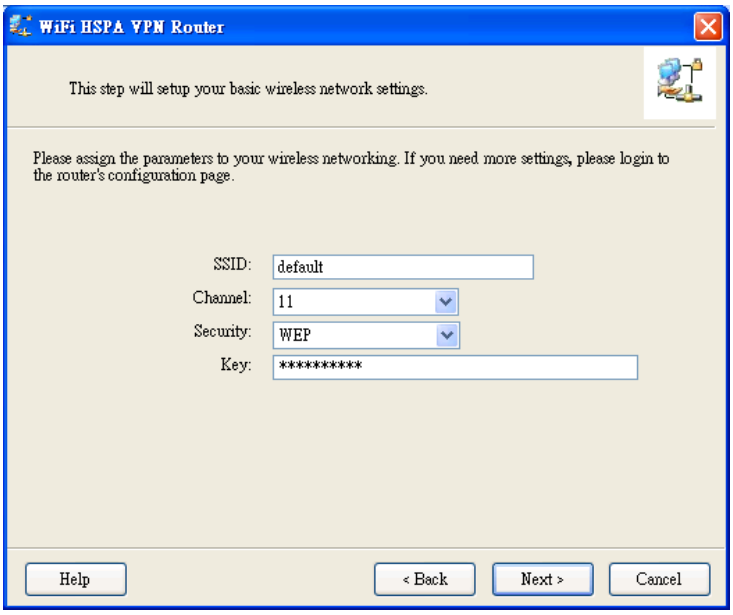
Click “Next” for continues


WiFi HSPA VPN Router
Prepare Setup
This step will make sure connection can be established between your PC and Router
Please make sure the following items.
1. Make sure the Router is powered on.
2. Make sure your network adapter is connected to the LAN port of the Router.
3. Make sure your network adapter has an IP address.
Help
< Back
Next >
Cancel

Step 5. Wireless Setting.
Select Wireless Enable or Disable, then click “Next” for continues.

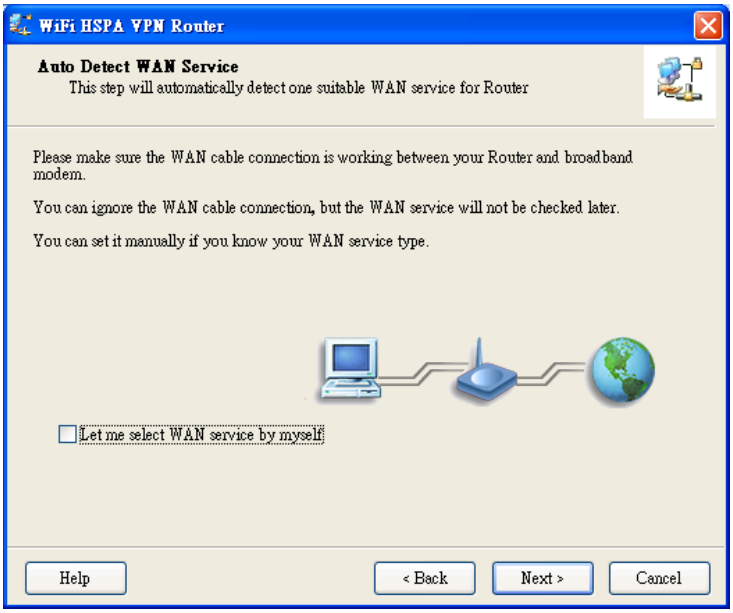

WiFi HSPA VPN Router
This step will setup your basic wireless network settings.
This will provide you with a basic workable setting for your wireless. You can also select to do it later.
Wireless:
Enable
Do not set at this time.
Help
< Back
Next >
Cancel

Step 6. Wireless Setting.
Key in the SSID, Channel and Security options, and then click “Next” for continues.

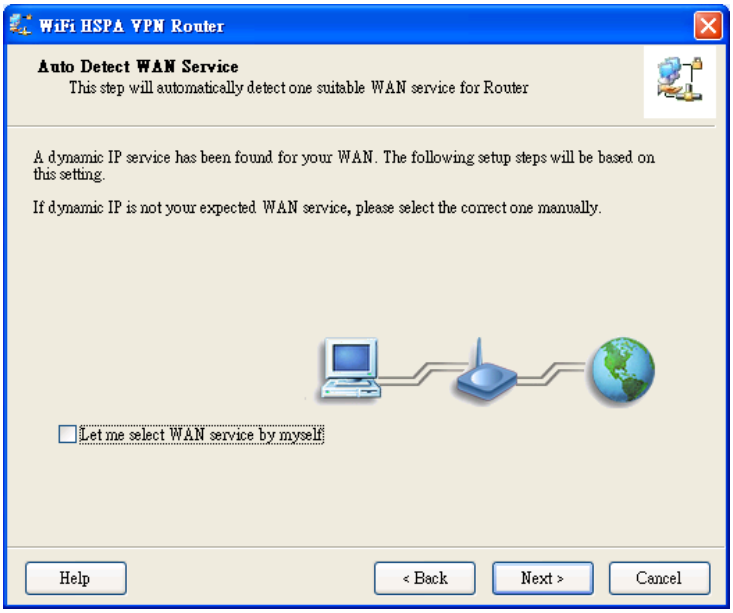


Step 7. Auto Detect WAN Service.
Click “Next” for continue.
Click the button, “Let me select WAN service by myself”, to disable this function.

Note: The Item supports to detect the Dynamic and PPPoE WAN Services only

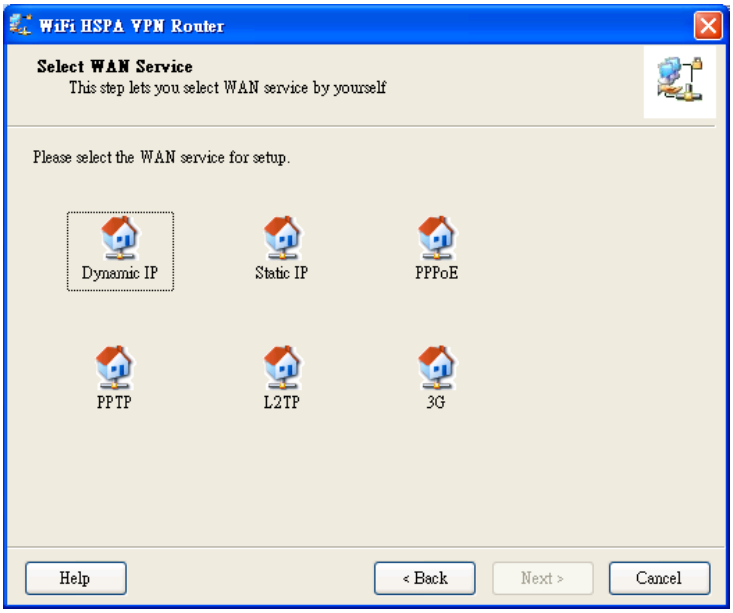

WiFi HSPA VPN Router
Auto Detect WAN Service
This step will automatically detect one suitable WAN service for Router
Please make sure the WAN cable connection is working between your Router and broadband modem.
You can ignore the WAN cable connection, but the WAN service will not be checked later.
You can set it manually if you know your WAN service type.
Let me select WAN service by myself
Help
< Back
Next >
Cancel

Example, the Dynamic WAN type is detected.


WiFi HSPA VPN Router
Auto Detect WAN Service
This step will automatically detect one suitable WAN service for Router
A dynamic IP service has been found for your WAN. The following setup steps will be based on this setting.
If dynamic IP is not your expected WAN service, please select the correct one manually.
Let me select WAN service by myself
Help
< Back
Next >
Cancel

Step 8. Manual select WAN Service

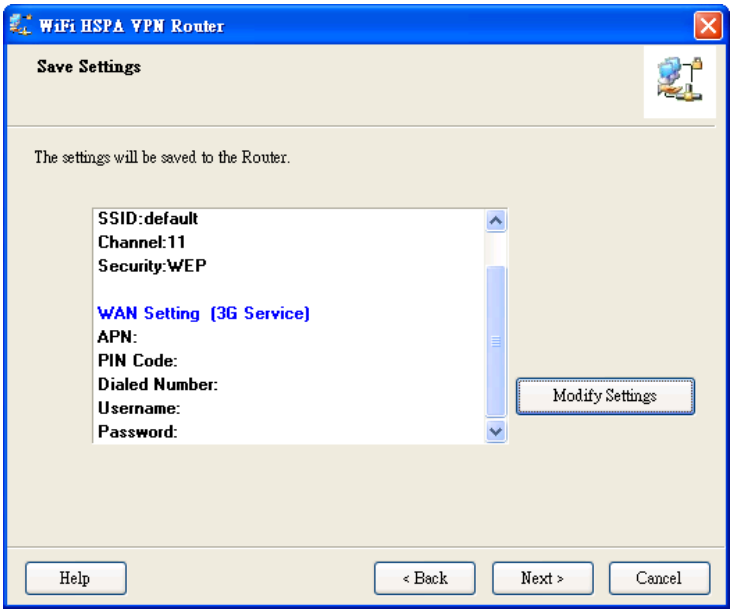
In the manual mode, Click the any icons for continues.



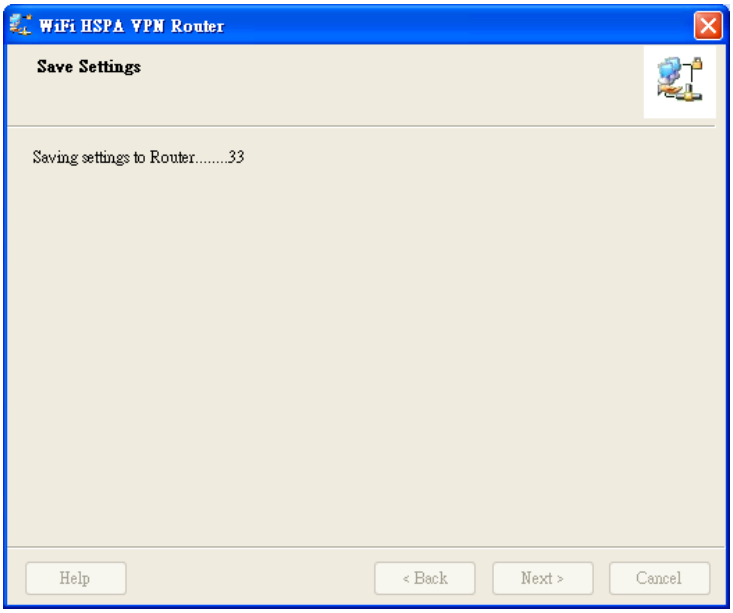
Example, 3G WAN Service:

Please fill in 3G service information which is provided by your ISP.

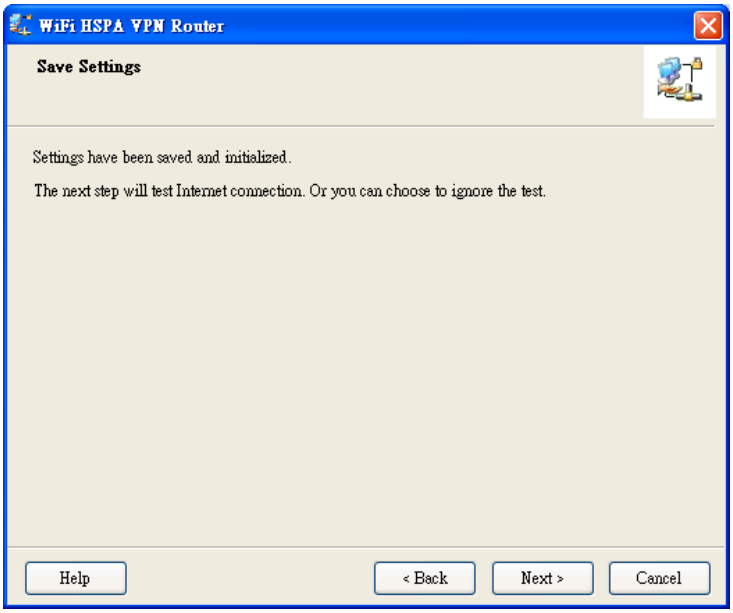
Step 9. Summary of the settings.
Click “Next” for continue.



Step 10. Reboot
The 802.11n Wireless HSPA VPN Router is rebooted.

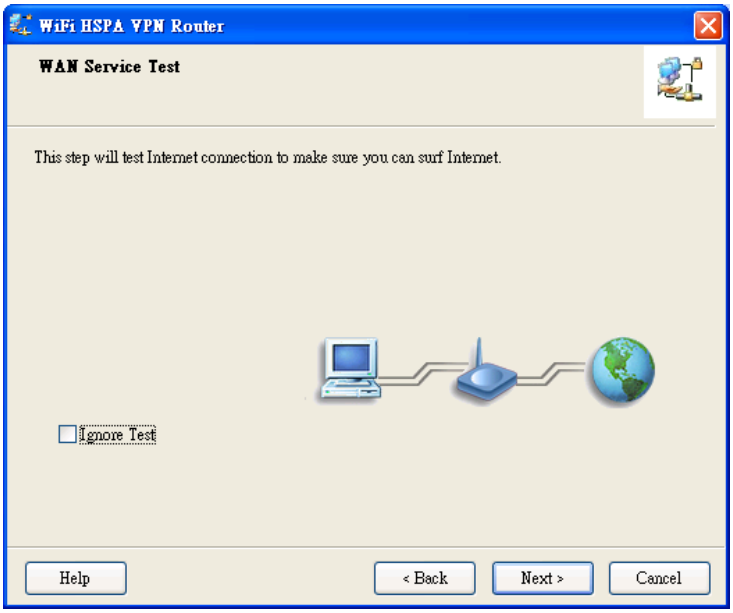


Step 11. Applied the Settings.
Click “Next” for continue.


WiFi HSPA VPN Router
Save Settings
Settings have been saved and initialized.
The next step will test Internet connection. Or you can choose to ignore the test.
Help
< Back
Next >
Cancel

Step 12. Test the Internet connection.
Test WAN Networking service. Click “Next” for continue.

You can ignore the by select the “Ignore Test”.


WiFi HSPA VPN Router
WAN Service Test
This step will test Internet connection to make sure you can surf Internet.
Ignore Test
Help
< Back
Next >
Cancel

Step 13. Setup Completed.

1. The EzSetup is finish; you can open the default web browser to configure advanced settings of the 802.11n Wireless HSPA VPN Router.

2. Click “Finish” to complete the installation.

WiFi HSPA VPN Router
Setup Completed
The Router is configured, but the WAN service functionality has not been checked.
Finish

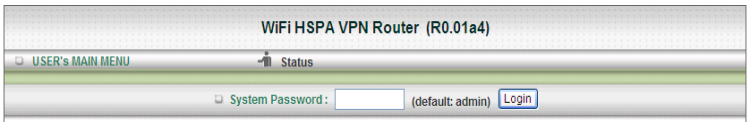
Chapter 3 Making Configuration

3.1 Web Wizard

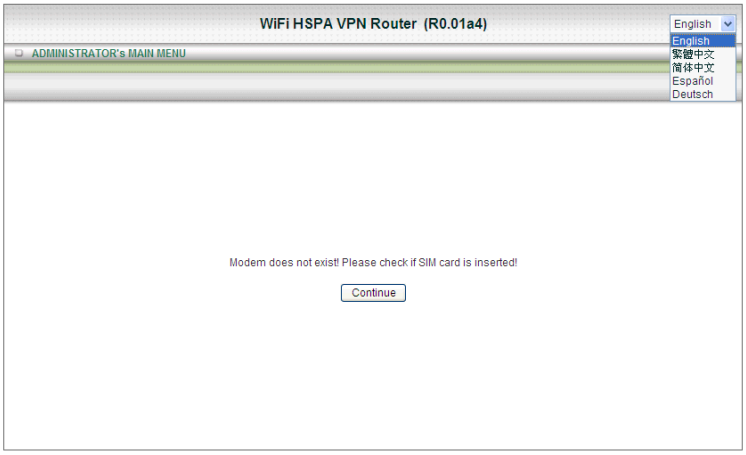
Type in the IP Address (http://192.168.123.254)

Welcome to AMIT - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://192.168.123.254
mywebsearch Search Smiley Central Screensavers
Art Design LCD CPU PDA Get More Hits Harddisk

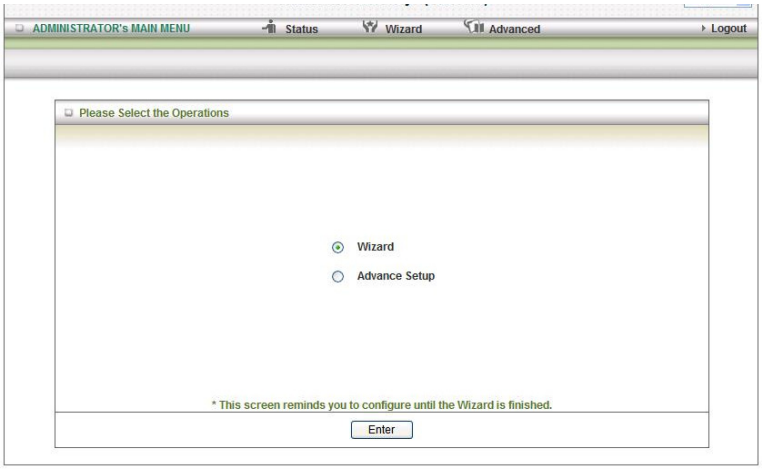
Type Password, the default is “admin” and click ‘login’ button.



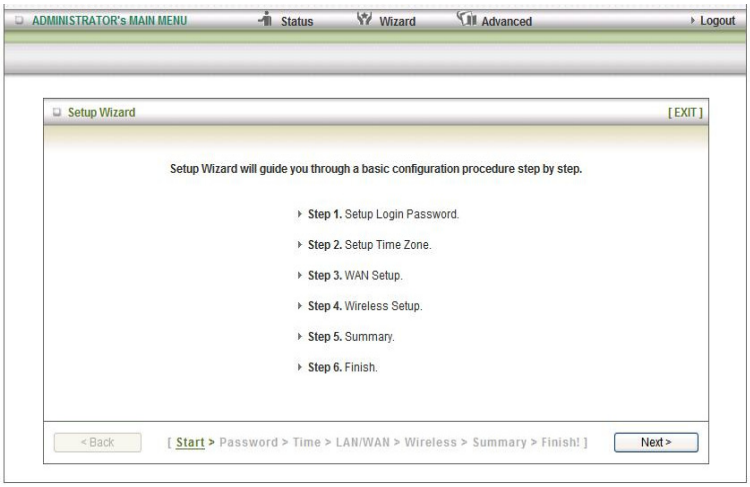
Select your language.



Press “Wizard” for basic settings with simple way.

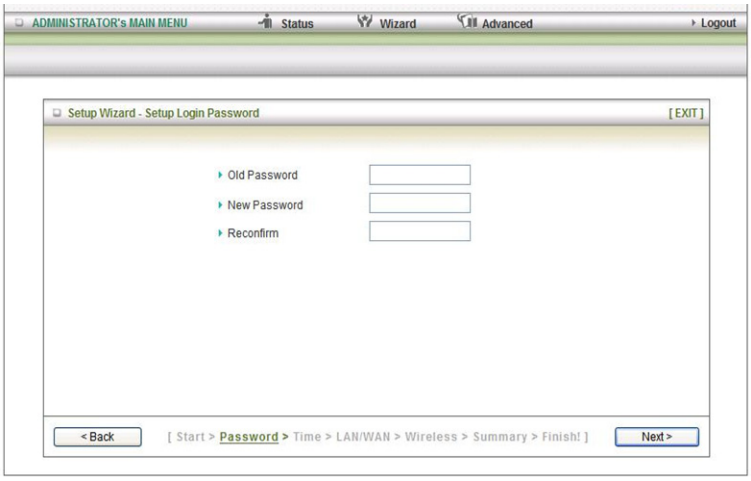


Press “Next” to start wizard.

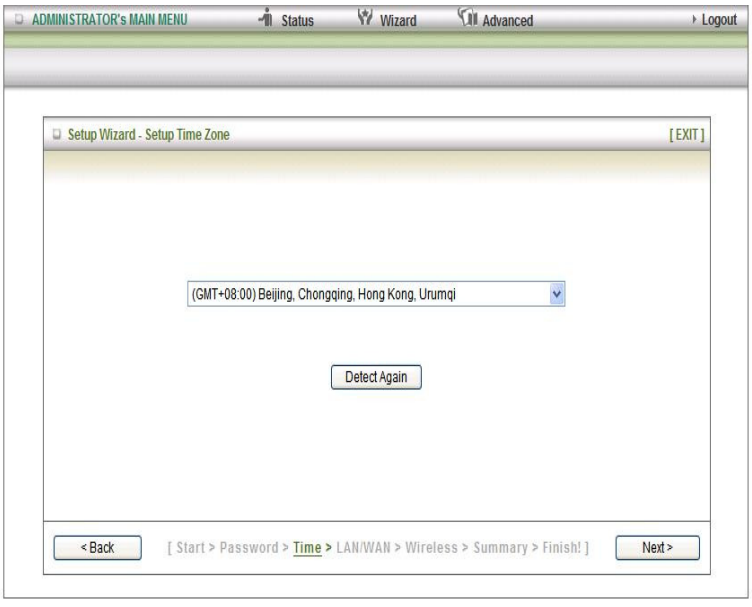


wizard

Step 1:
Set up your system password.

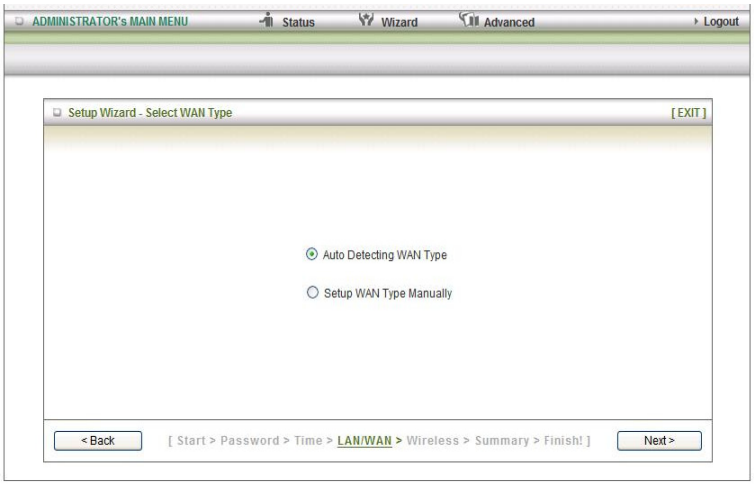


Step 2:
Select Time Zone.

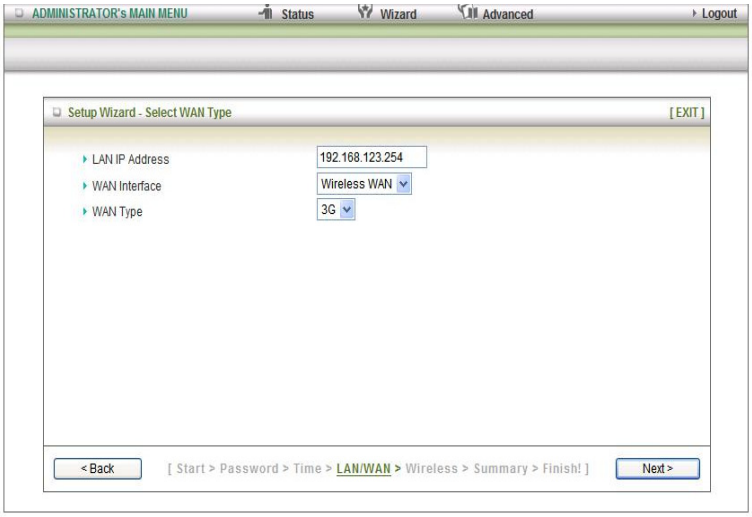


Step 3:
Select Wan Type.

Auto Detecting or
Setup Manually.

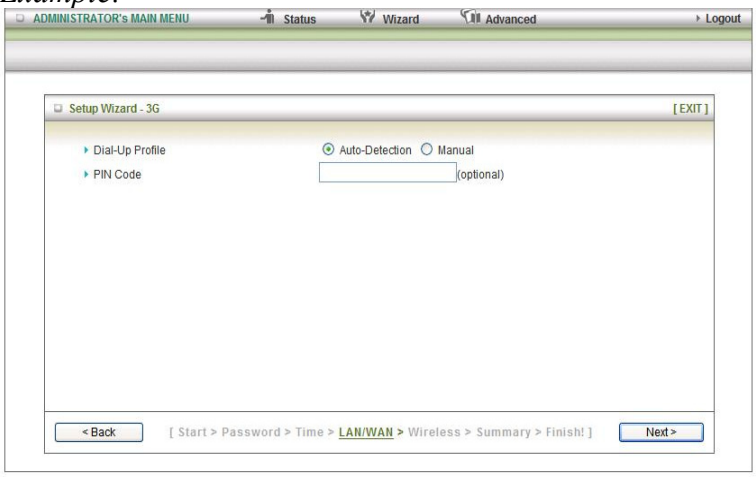


Setup the LAN IP and WAN Type.

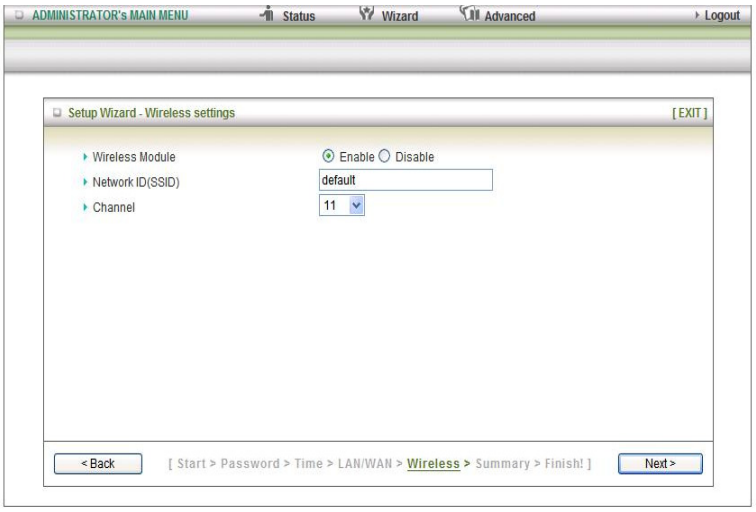


Example:

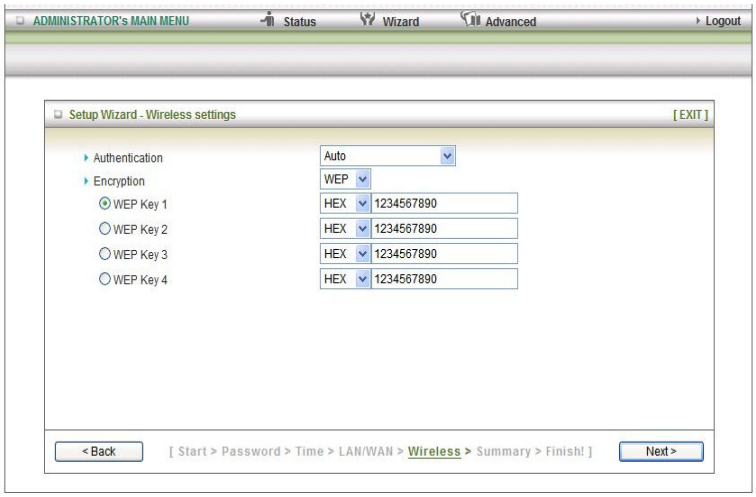
Step 4:
Please fill in 3G service information which is provided by your ISP.



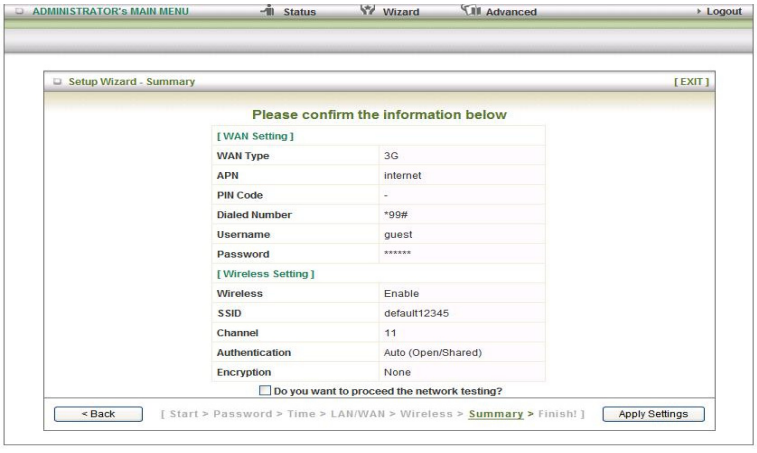
Step 5:
Set up your Wireless.



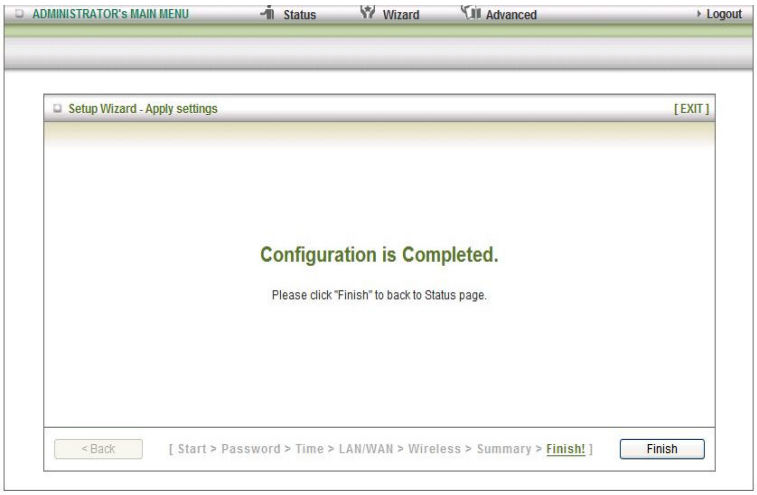
Set up your Authentication and Encryption.



Step 6:
Then click Apply Setting.
And then the device will reboot.

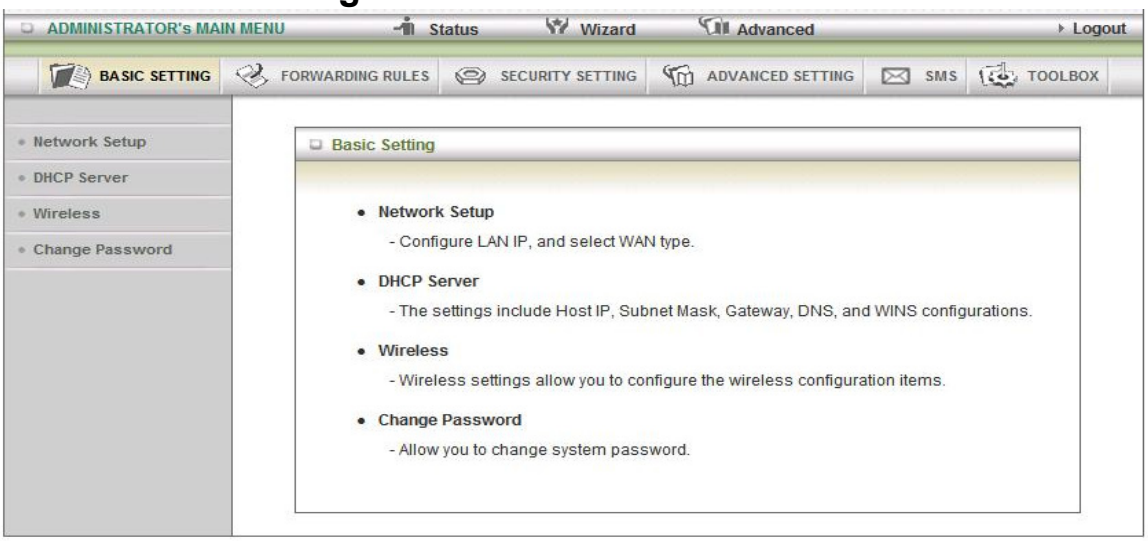


Step 7:
Click Finish to complete it.

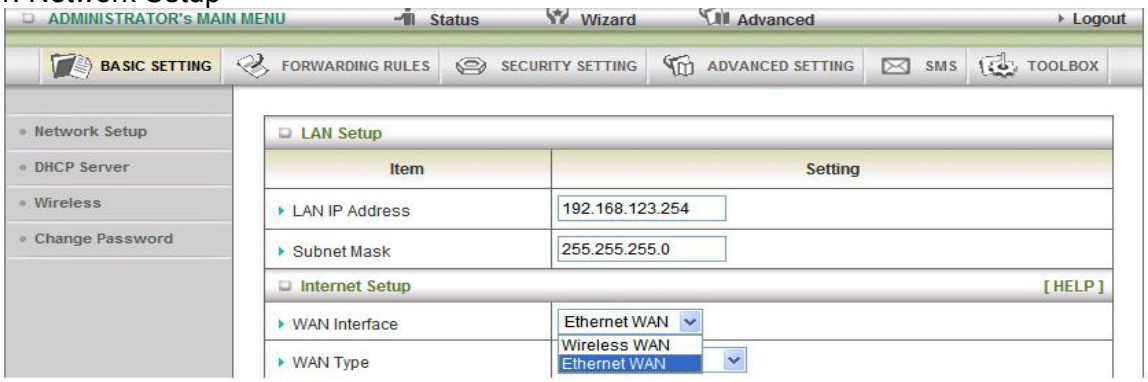


3.2 Advanced Setting

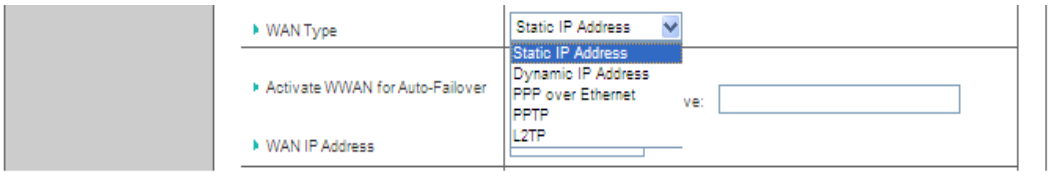
3.2.1 Basic Setting



1. Network Setup

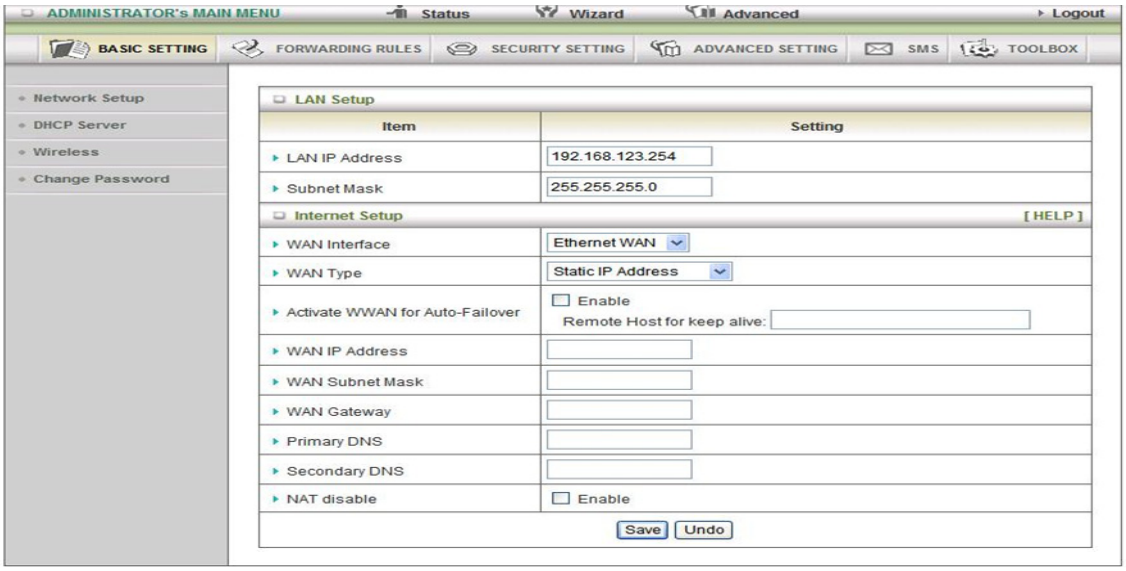


1. **LAP IP Address:** the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Router. You can change it if necessary.
2. **Subnet Mask: insert 255.255.255.0**
3. **WAN Interface:** Select Ethernet WAN or Wireless WAN to continue.



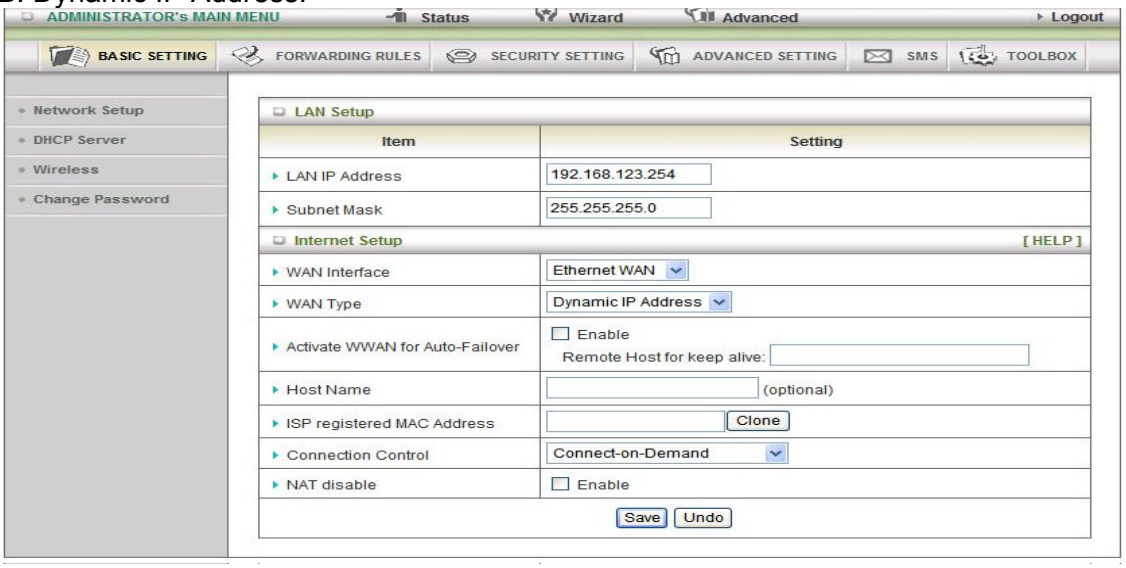
4. **WAN Type**: WAN connection type of your ISP. You can click WAN Type Combo button to choose a correct one from the following options:

A. Static IP Address:



WAN IP Address, Subnet Mask, Router, Primary and Secondary DNS: enter the proper setting provided by your ISP.

B. Dynamic IP Address:



1. Active WWAN for Auto-Failover: The WAN type will be change to wireless-WAN automatically, if the wired-WAN is defunct.
2. Host Name: optional, required by some ISPs, for example, @Home.
3. ISP register MAC address: You can change the WAN port MAC address, it is your ISP assigned to you.
4. Connection Control: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send

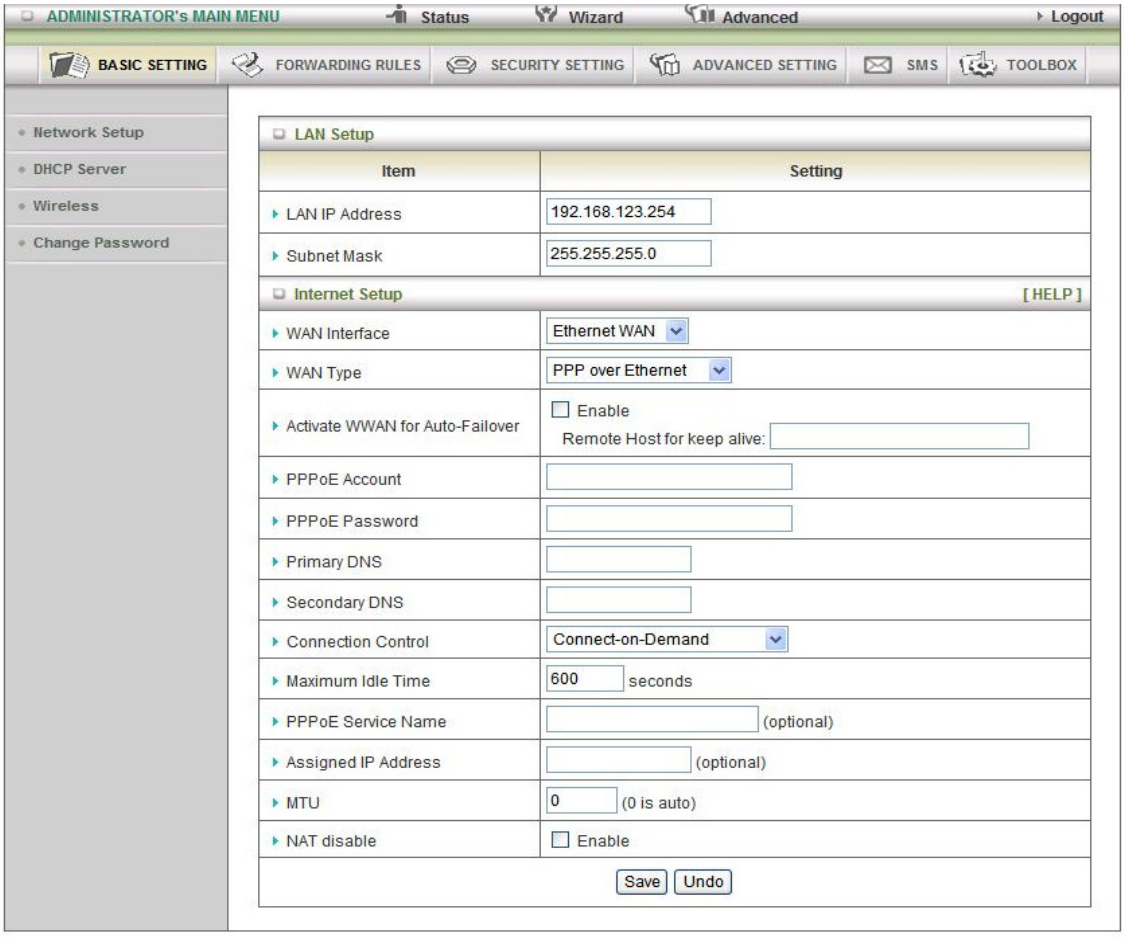
outgoing packets.

Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

5. NAT disable**:** the option bridges data form WAN port to LAN port.

C. PPP over Ethernet



1. Active WWAN for Auto-Failover: The WAN type will be change to wireless-WAN automatically, if the wired-WAN is defunct.
2. PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.
3. Primary DNS/ Secondary DNS: This feature allows you to assign a Primary/Secondary DNS Server, contact to your ISP to get it.
4. Connection Control: There are 3 modes to select:

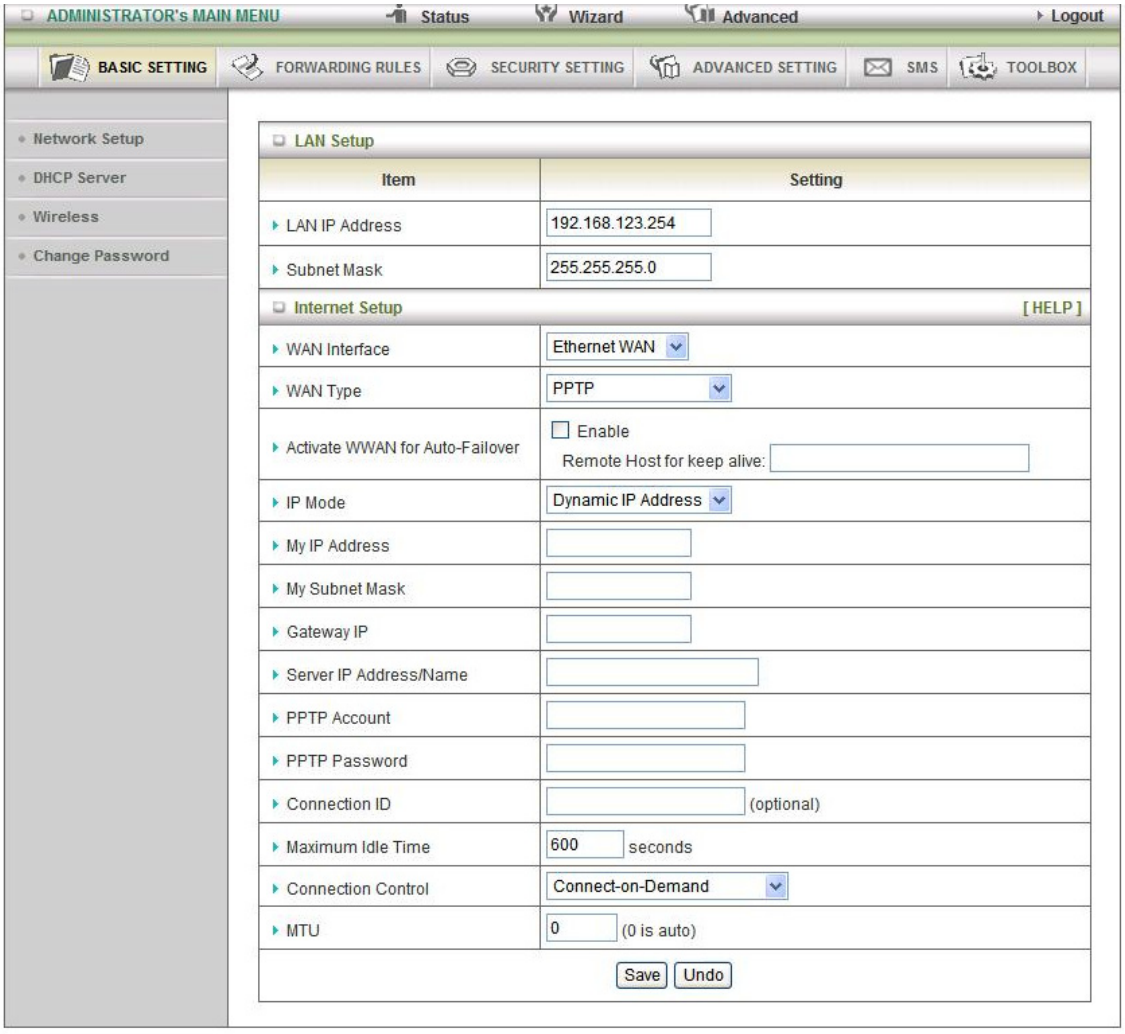
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

5. Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable "Auto-reconnect" to disable this feature.
6. PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
7. Assigned IP address: Optional, Input the IP address you want. Usually, leave it blank.
8. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).
9. NAT disable: the option bridges data form WAN port to LAN port

D. PPTP

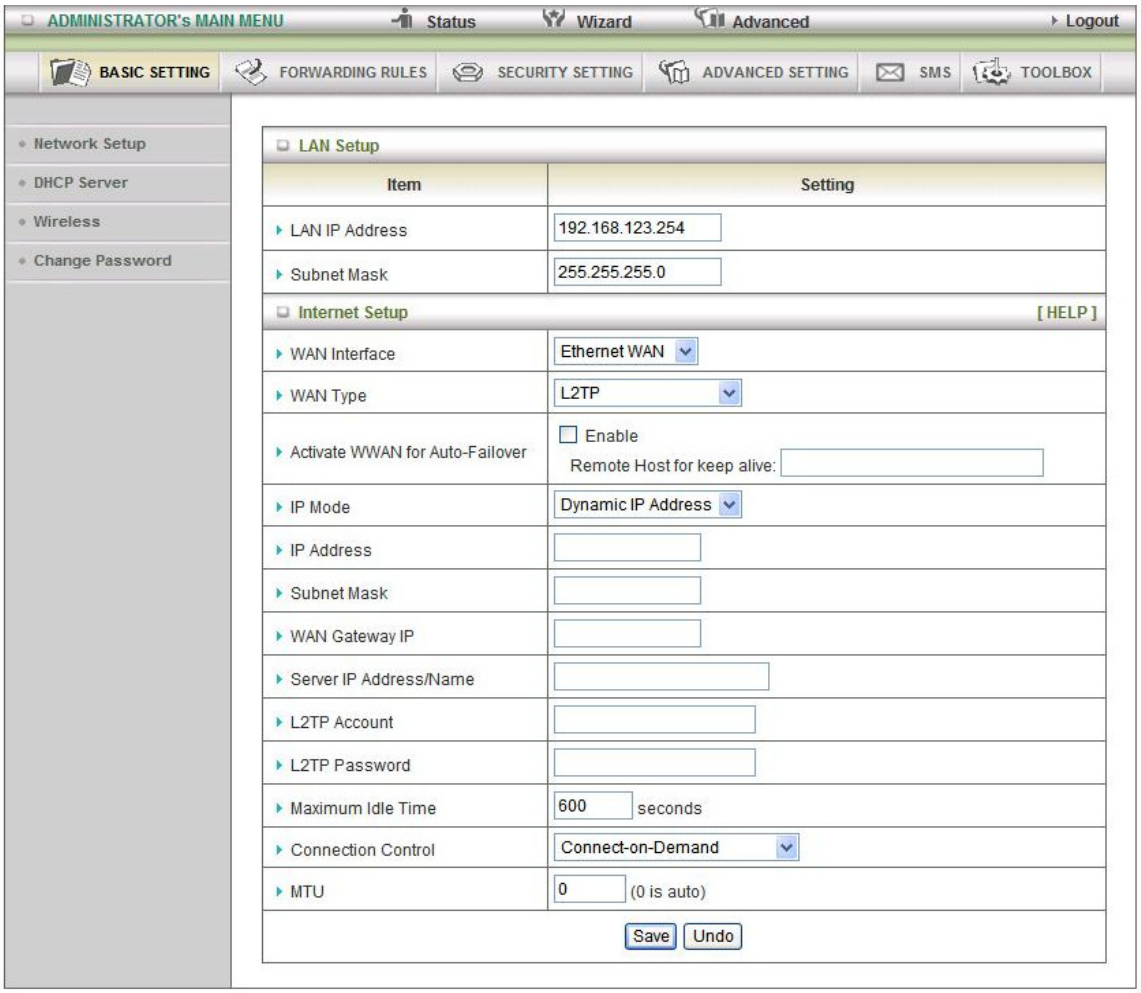


First, please check your ISP assigned and select the IP Mode - Static IP Address or Dynamic IP

Address. For example: Use Static, the private IP address, subnet mask and Router are your ISP assigned to you.

1. Active WWAN for Auto-Failover: The WAN type will be change to wireless-WAN automatically, if the wired-WAN is defunct.
2. My IP Address, My Subnet Mask and WAN Router IP: the private IP address, subnet mask and Router IP your ISP assigned to you.
3. Server IP Address/Name: the IP address or URL of the PPTP server.
4. PPTP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
5. Connection ID: optional. Input the connection ID if your ISP requires it.
6. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable “Auto-reconnect” to disable this feature. If Auto-reconnect is enabled, this product will connect with ISP automatically, after system is restarted or connection is dropped.
7. Connection Control: There are 3 modes to select:
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.
   Auto Reconnect (Always-on): The device will link with ISP until the connection is established. Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
8. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).

E. L2TP

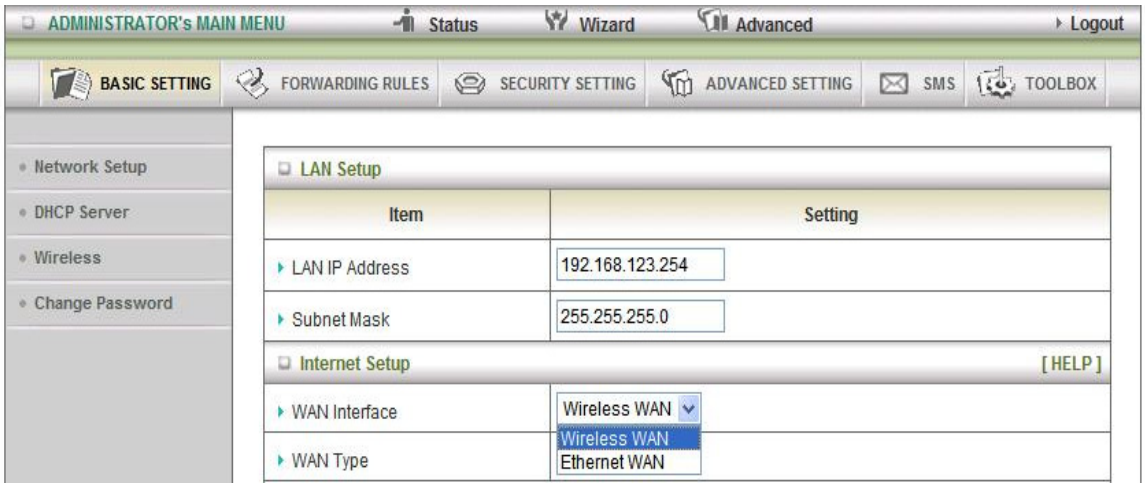


First, please check your ISP assigned and select the IP Mode - Static IP Address or Dynamic IP Address. For example: Use Static, the private IP address, subnet mask and Router are your ISP assigned to you.

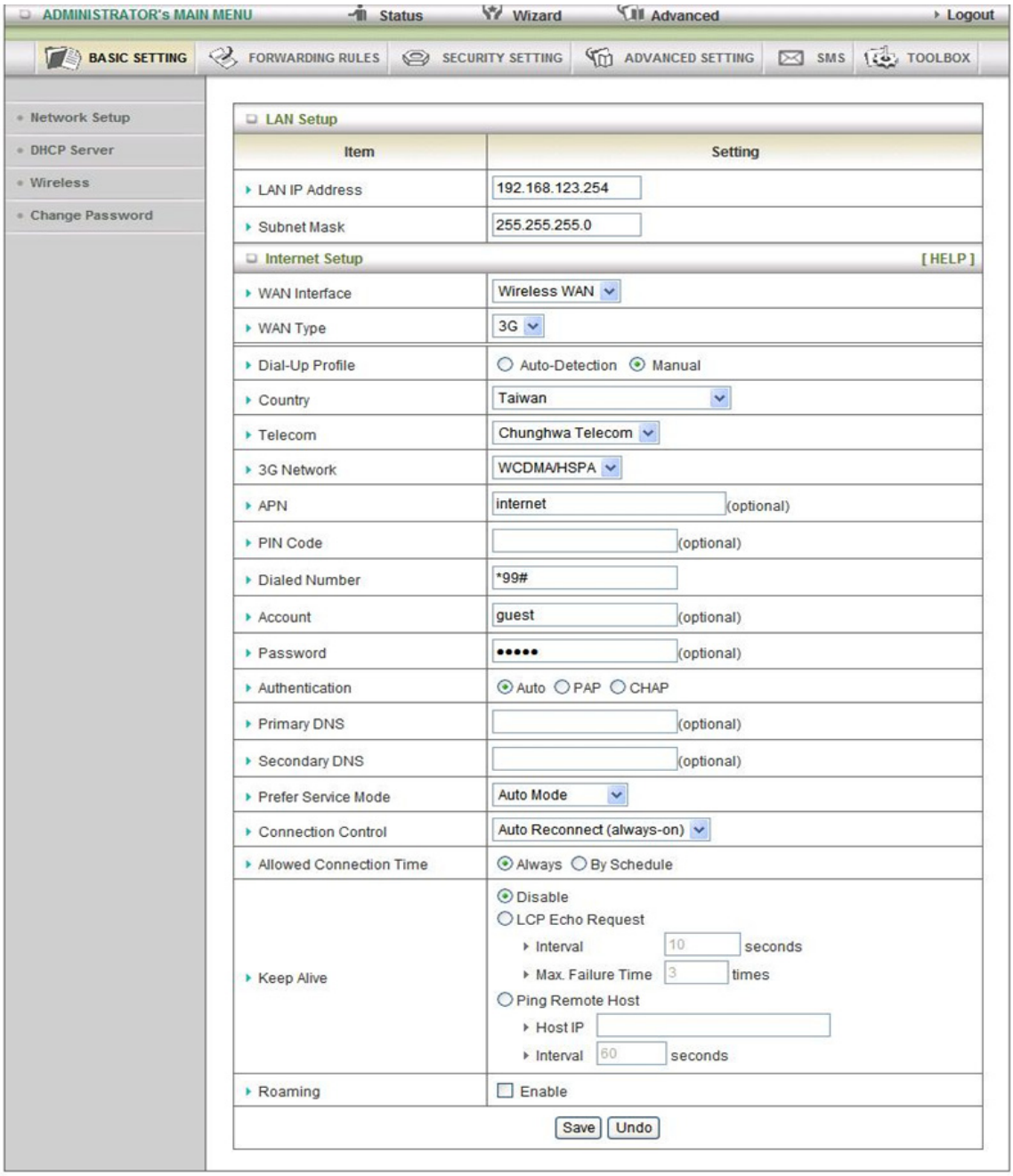
1. Activate WWAN for Auto-Failover: The WAN type will be change to wireless-WAN automatically, if the wired-WAN is defunct.
2. IP Address, Subnet Mask and WAN Router IP: the private IP address, subnet mask and Router IP your ISP assigned to you.
3. Server IP Address/Name: the IP address or URL of the PPTP server.
4. L2TP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
5. Maximum Idle Time: the time of no activity to disconnect your L2TP session. Set it to zero or enable “Auto-reconnect” to disable this feature. If Auto-reconnect is enabled, this product will connect with ISP automatically, after system is restarted or connection is dropped.

6. Connection Control: There are 3 modes to select:
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.
   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.
   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
7. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).

Or select Wireless WAN for 3G Setting.



F. 3G



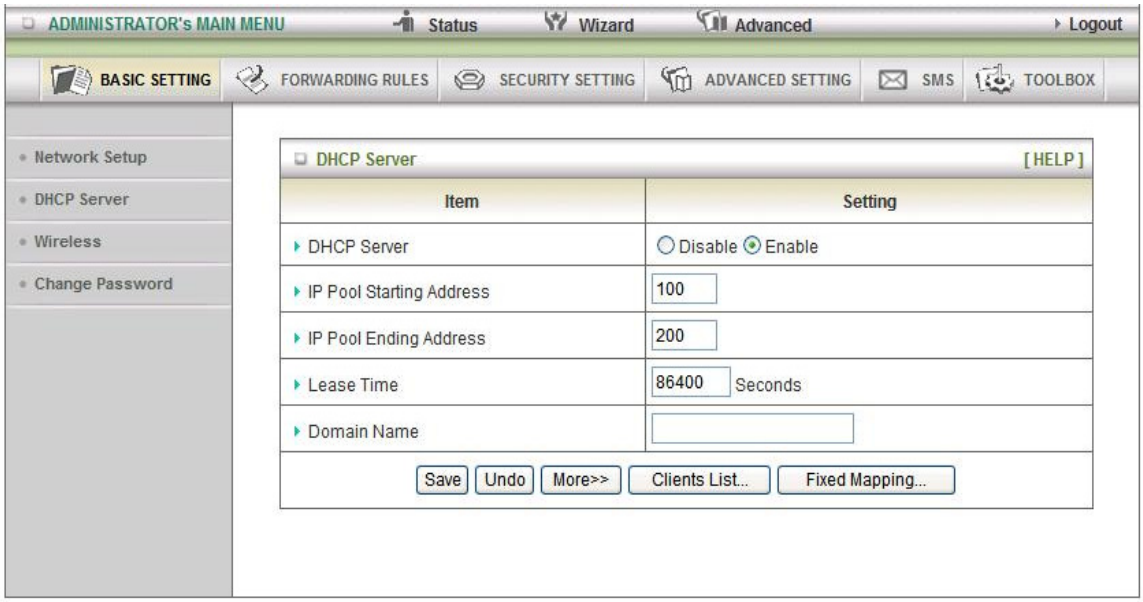
For 3G WAN Networking. The WAN fields may not be necessary for your connection. The information on this page will only be used when your service provider requires you to enter a User Name and Password to connect with the 3G network.

Please refer to your documentation or service provider for additional information.

1. Dial-Up Profile: select auto or manual to continue.
2. Country: select your country.
3. Telecom: select your telecom.

4. 3G Network: select the 3G Network.
5. APN: Enter the APN for your PC card here.(Optional)
6. Pin Code: Enter the Pin Code for your SIM card(Optional)
7. Dial-Number: This field should not be altered except when required by your service provider.
8. Account: Enter the new User Name for your PC card here, you can contact to your ISP to get it.
9. Password: Enter the new Password for your PC card here, you can contact to your ISP to get it.
10. Authentication: Choose your authentication.
11. Primary DNS: This feature allows you to assign a Primary DNS Server, contact to your ISP to get it.
12. Secondary DNS: This feature allows you to assign a Secondary DNS Server, you can contact to your ISP to get it.
13. Connection Control: select your connection control
14. Keep Alive: you can diagnose your connection by it.

2. DHCP Server



Press **"More>>",**

1. **DHCP Server:** Choose either **Disable** or **Enable**
2. **Lease Time:** DHCP lease time to the DHCP client
3. **IP Pool Starting/Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool
4. **Domain Name:** Optional, this information will be passed to the client
5. **Primary DNS/Secondary DNS:** Optional, This feature allows you to assign a DNS Servers
6. **Primary WINS/Secondary WINS:** Optional, this feature allows you to assign a WINS Servers
7. **Router:** Optional, Router Address would be the IP address of an alternate Router.

This function enables you to assign another Router to your PC, when DHCP server offers an IP to your PC.

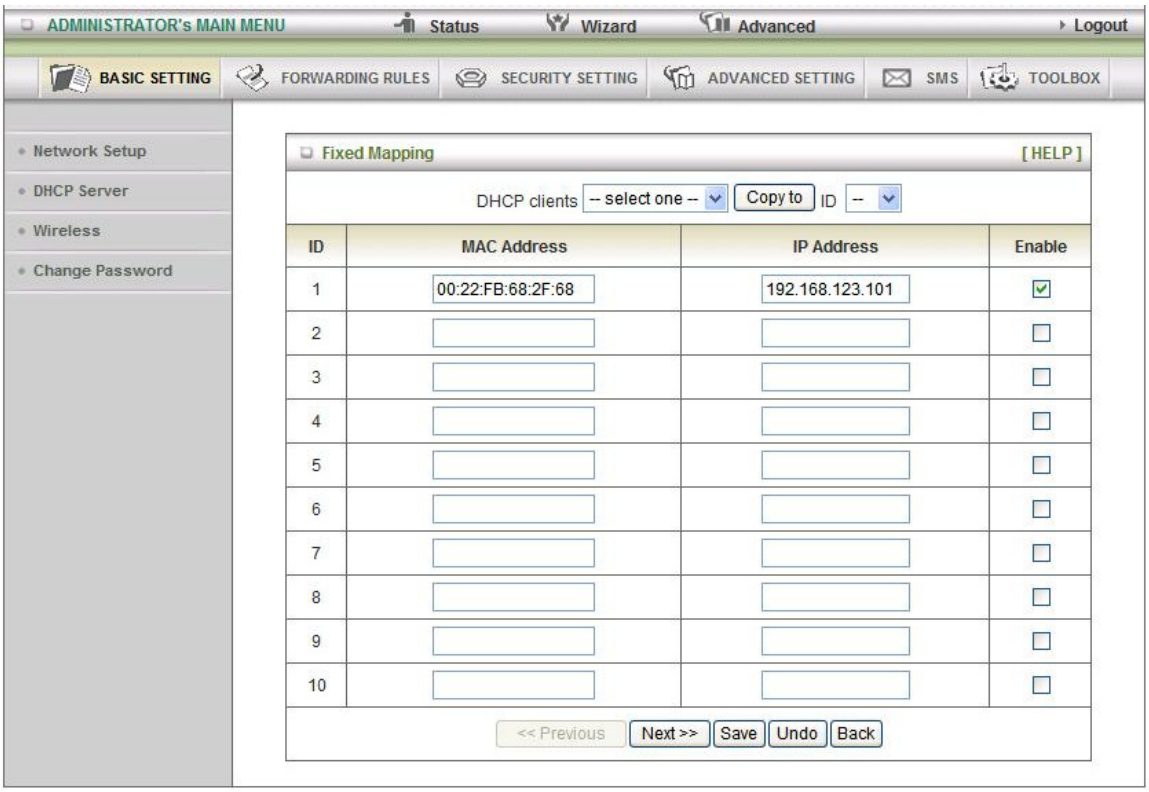
Click on "Save" to store your setting or click "Undo" to give up

DHCP Clients List

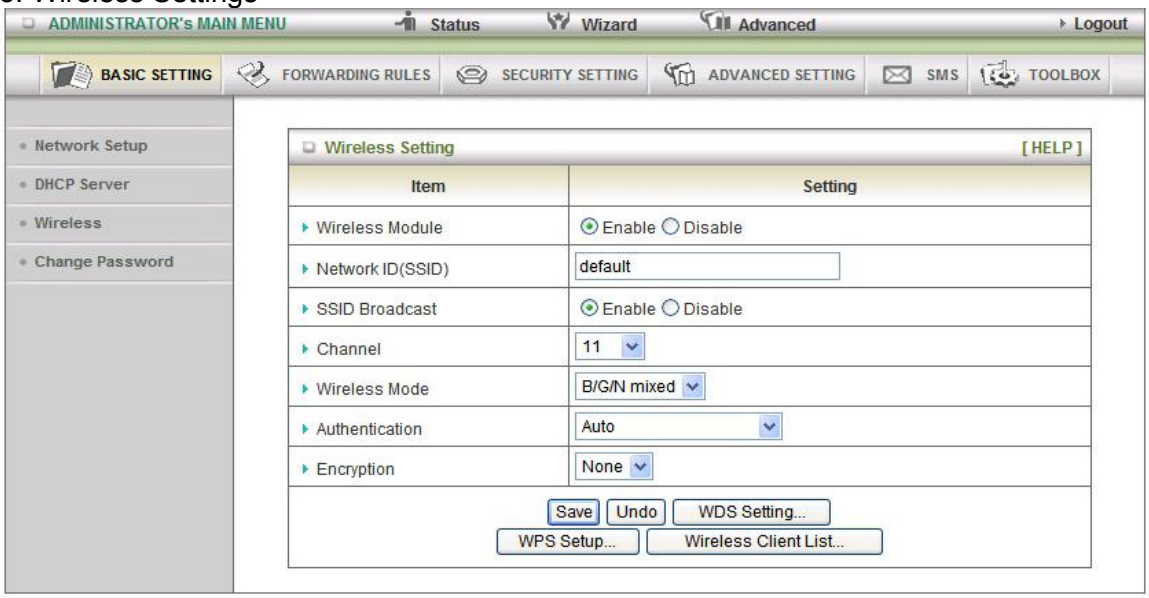
The list of DHCP clients shows here.

DHCP Fixed Mapping

The DHCP Server will reserve the special IP for special MAC address, shows below.



3. Wireless Settings



Wireless settings allow you to set the wireless configuration items.

1. **Wireless Module:** The user can enable or disable wireless function
2. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory setting is “default”)
3. **SSID Broadcast:** The router will broadcast beacons that have some information, including ssid so that wireless clients can know how many AP devices by scanning function in the network. Therefore, this function is disabled; the wireless clients can not find the device from beacons.
4. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain.

   The factory setting is channel 11.
5. **Wireless Mode:** Choose B/G Mixed, B only, G only, N only, G/N Mixed or B/G/N mixed. The factory default setting is B/G/N mixed.
6. **Authentication mode:** You may select from nine kinds of authentication to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, WPA /WPA2.

Open

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC

address is explicitly excluded in the AP/router configuration.

Shared

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

Auto

The AP will Select the Open or Shared by the client's request automatically.

WPA-PSK

Select Encryption and Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits.

If you select ASCII, the length of pre-share key is from 8 to 63.

Fill in the key, Ex 12345678

WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server IP address or the 802.1X server's domain-name.

Select Encryption and RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If you select ASCII, the length of pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA-PSK2

WPA-PSK2 user AES and TKIP for Same the encryption, the others are same the WPA-PSK.

WPA2

WPA2 add uses AES and TKIP for encryption, the others are same the WPA.

WPA-PSK/WPA-PSK2

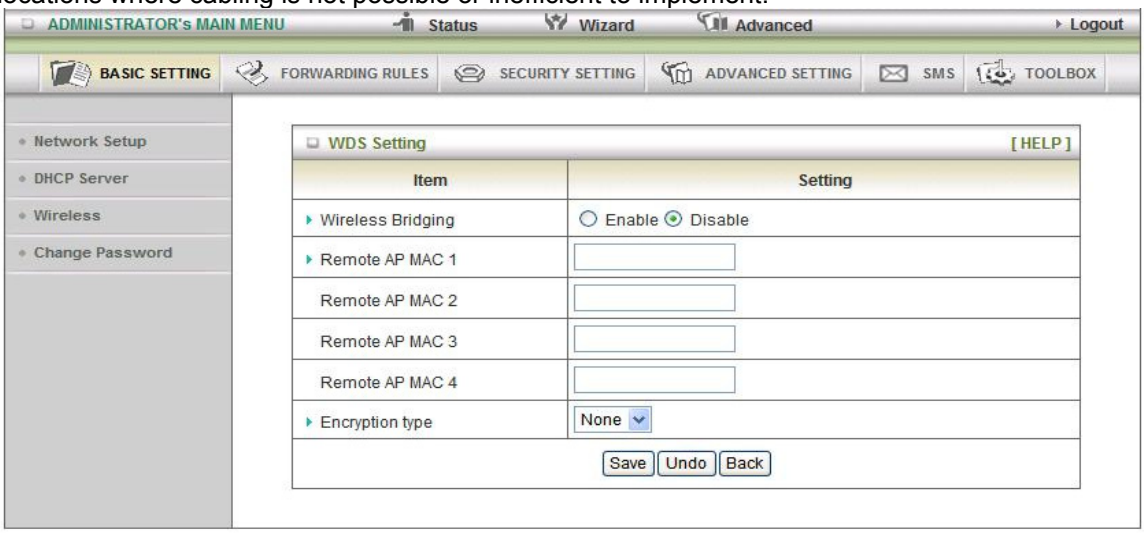
Another encryption options for WPA-PSK-TKIP and WPA-PSK2-AES, the others are same the WPA-PSK.

WPA/WPA2

Another encryption options for WPA-TKIP and WPA2-AES, the others are same the WPA.

WDS(Wireless Distribution System) Setting

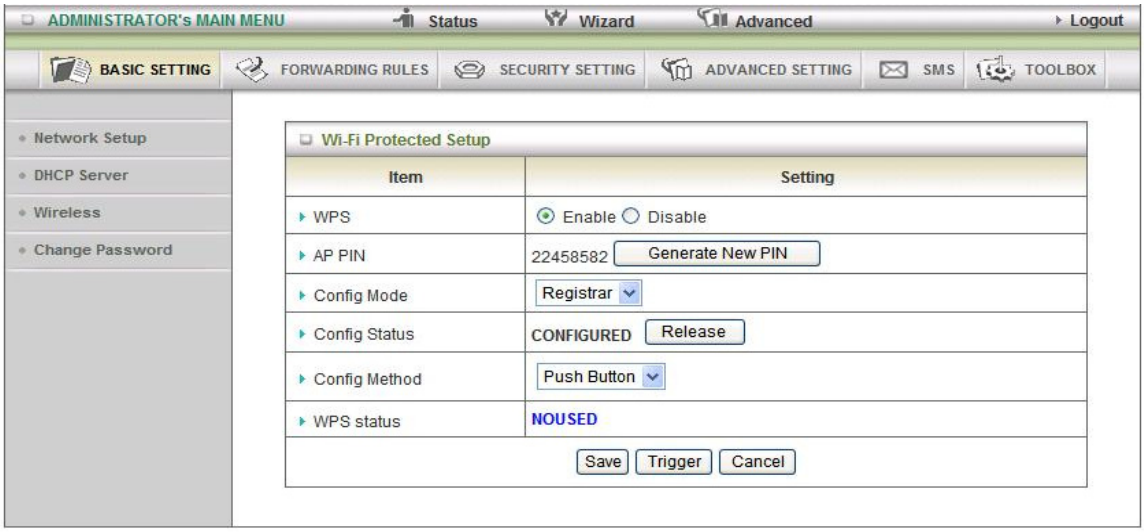
WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.



WPS (Wi-Fi Protection Setup)

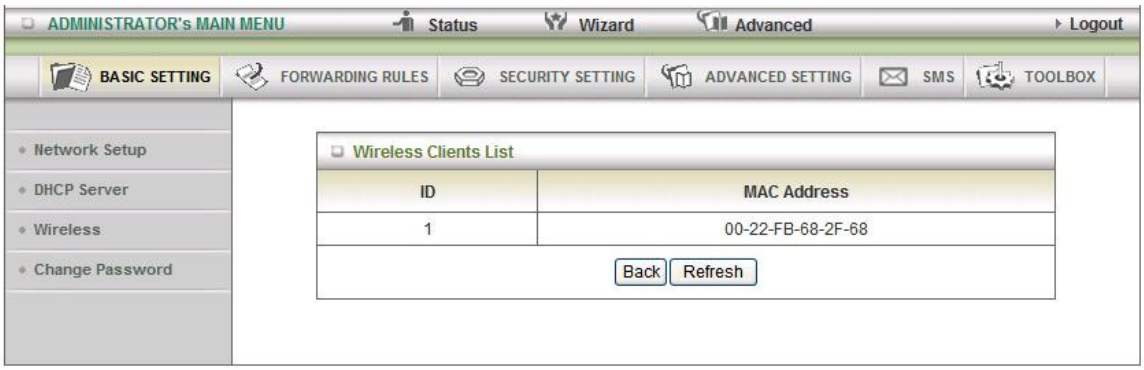
WPS is Wi-Fi Protection Setup which is similar to WCN-NET and offers safe and easy way in Wireless Connection.

Default value is “enable”

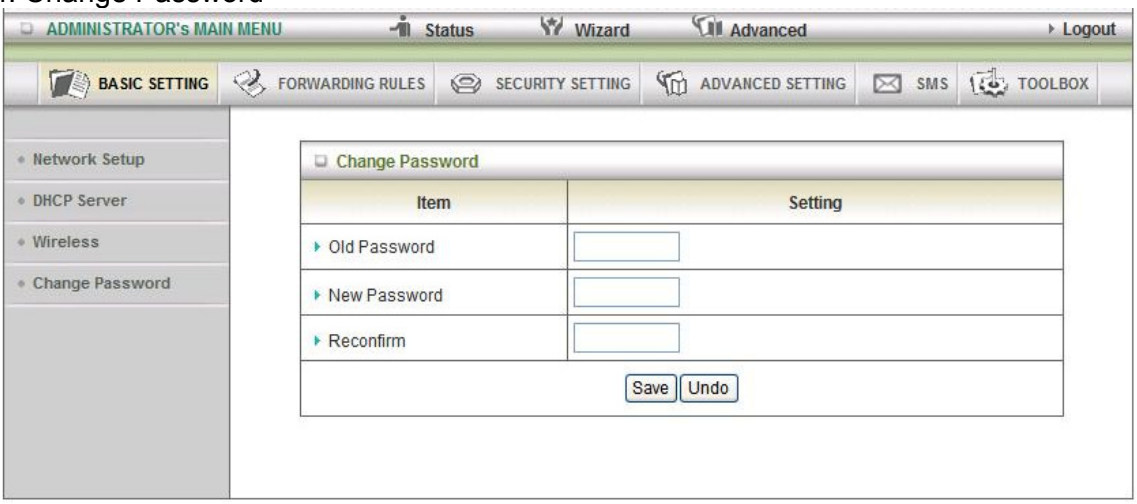


Wireless Client List

The list of wireless client is shows here.



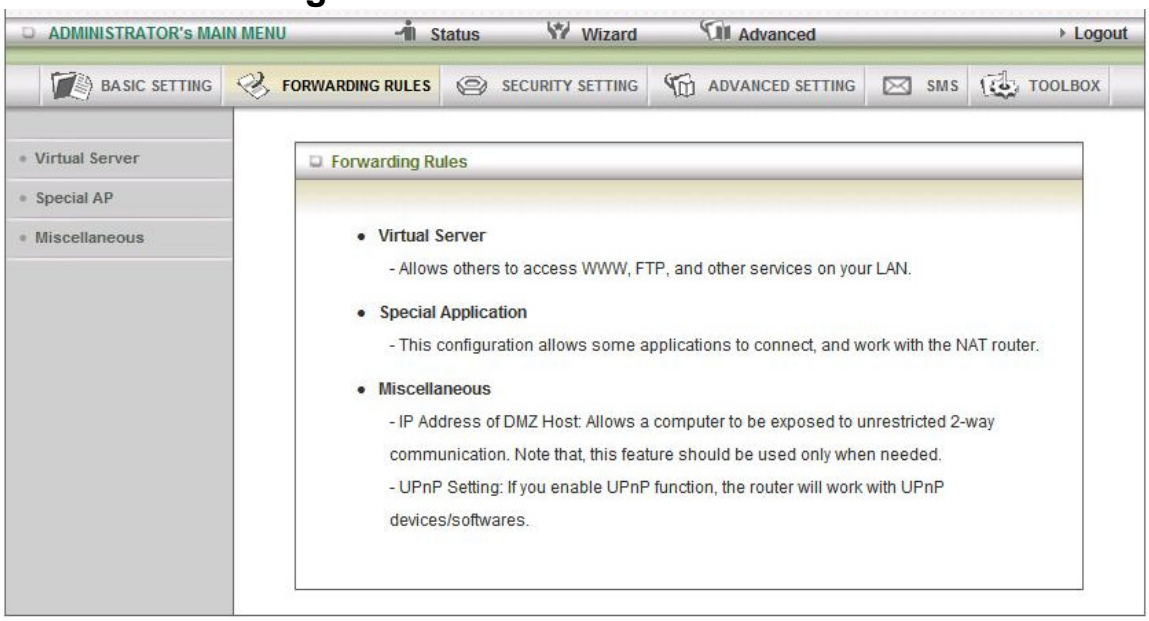
4. Change Password



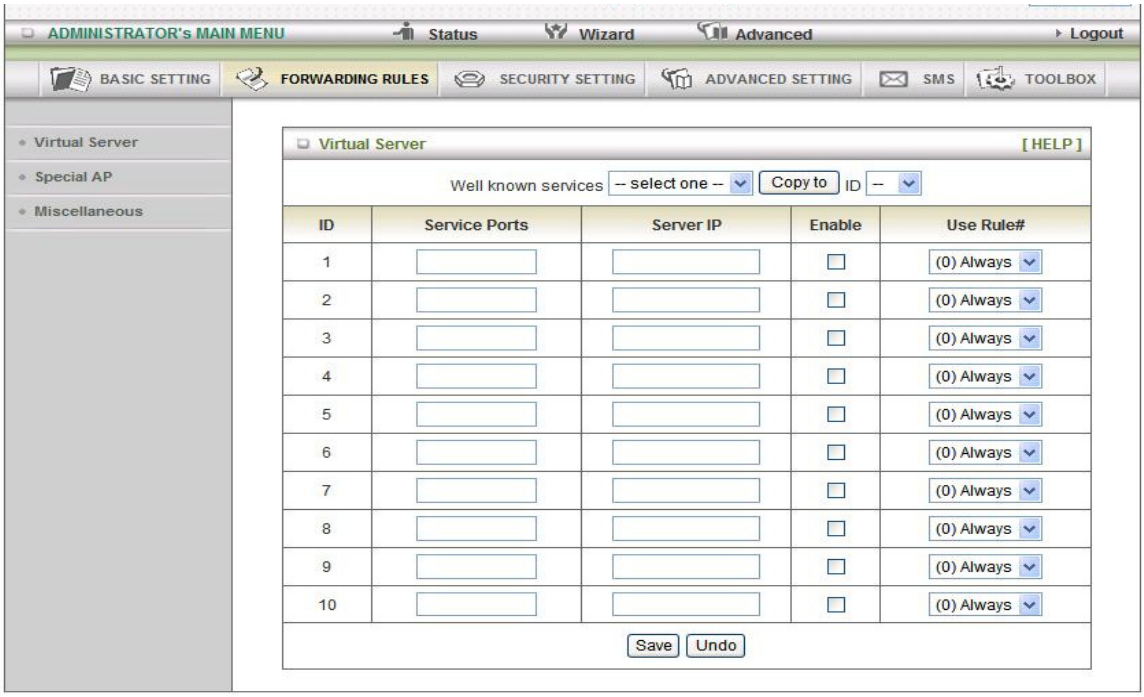
You can change Password here. We **strongly** recommend you to change the system password for security reason.

Click on “Save” to store your setting or “Undo” to give up

3.2.2 Forwarding Rules


ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
SMS
TOOLBOX
Virtual Server
Special AP
Miscellaneous
Forwarding Rules
Virtual Server
- Allows others to access WWW, FTP, and other services on your LAN.
Special Application
- This configuration allows some applications to connect, and work with the NAT router.
Miscellaneous
- IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.
- UPnP Setting: If you enable UPnP function, the router will work with UPnP devices/softwares.

1. Virtual Server



This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

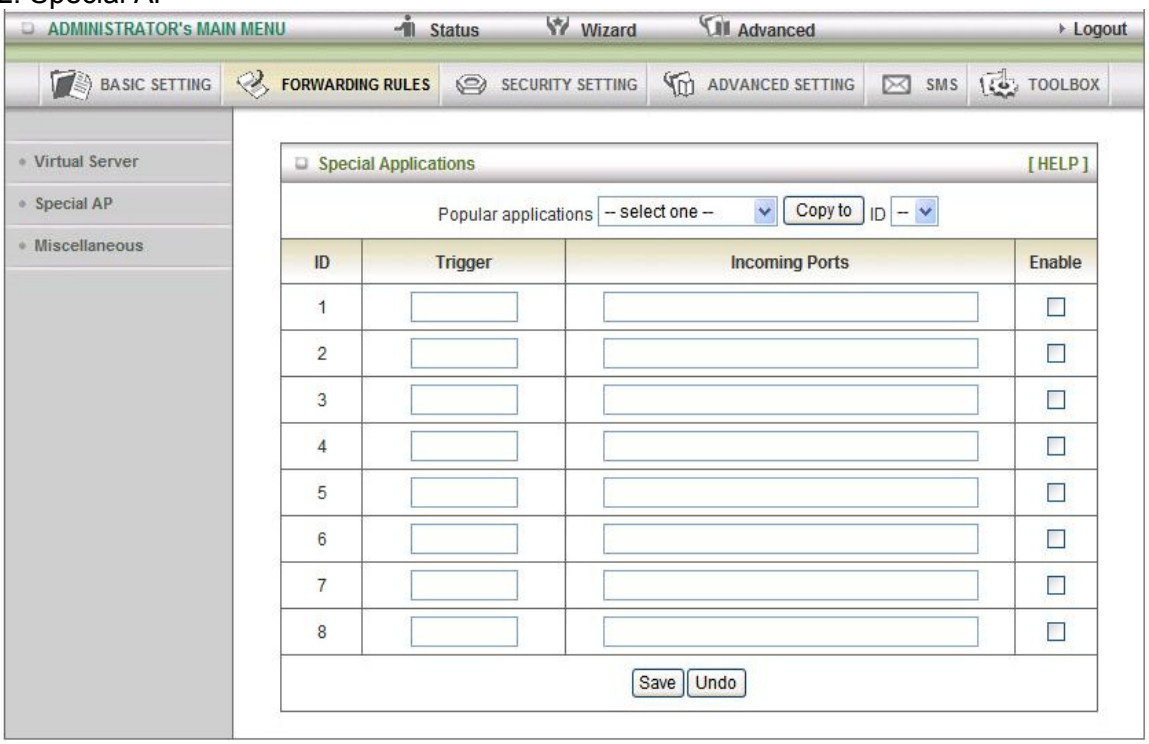
A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP. Virtual Server** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V

Click on "Save" to store your setting or "Undo" to give up

2. Special AP



Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. **The Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.

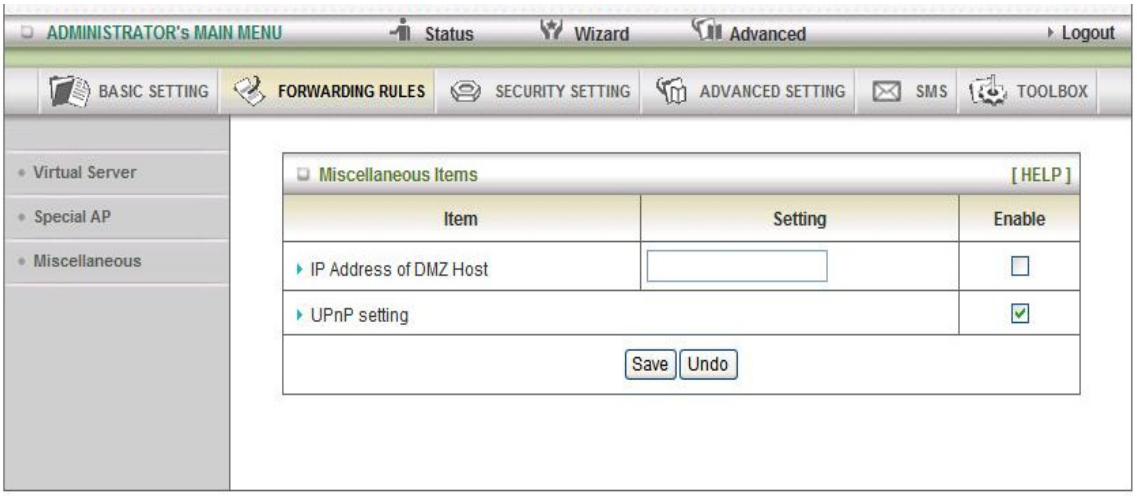
1. **Trigger:** the outbound port number issued by the application.

2. **Incoming Ports**: when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.
   This product provides some predefined settings.

   Select your application and Click "**Copy to"** to add the predefined setting to your list.

Click on "Save" to store your setting or" Undo" to give up

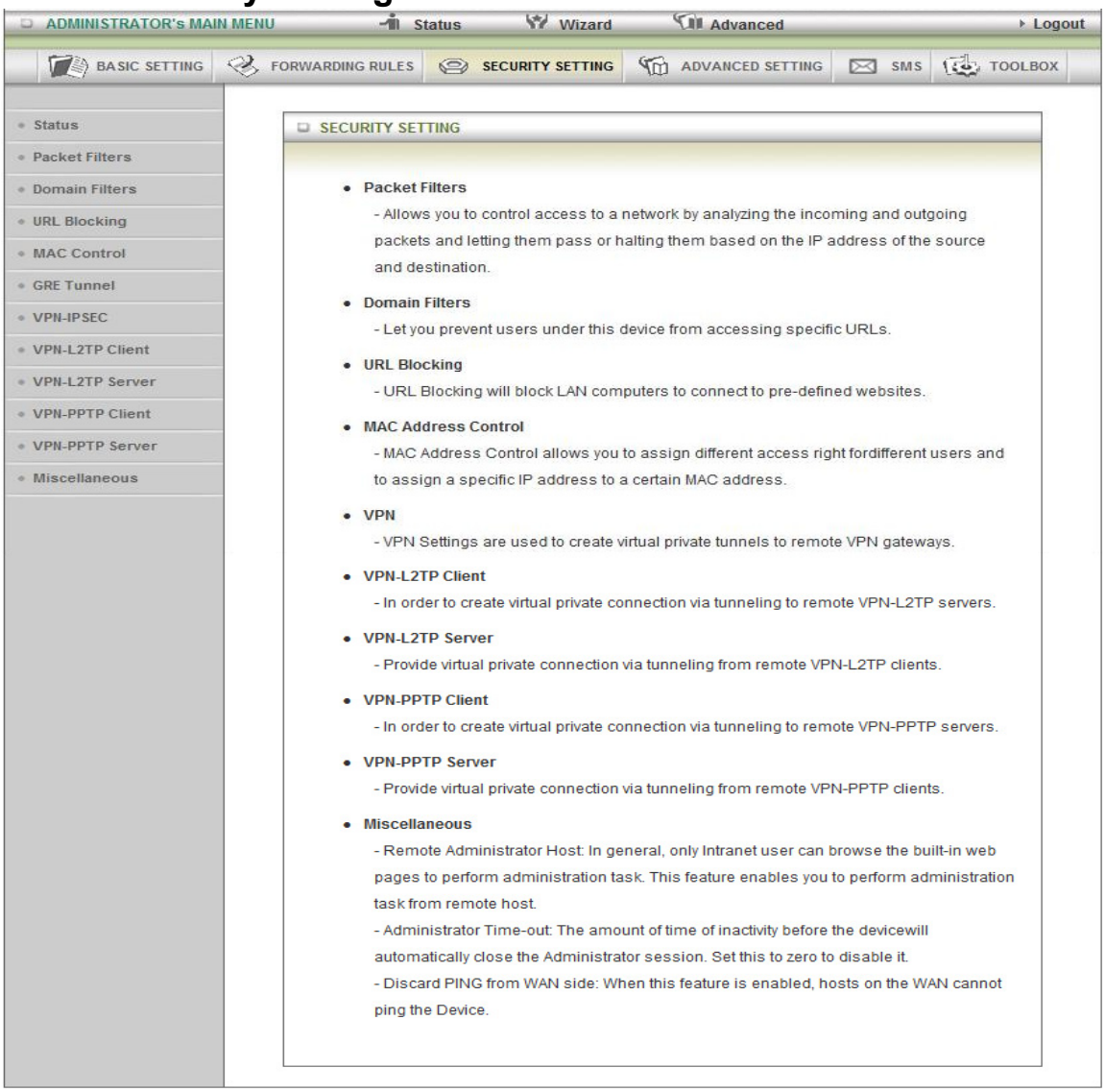
3. Miscellaneous



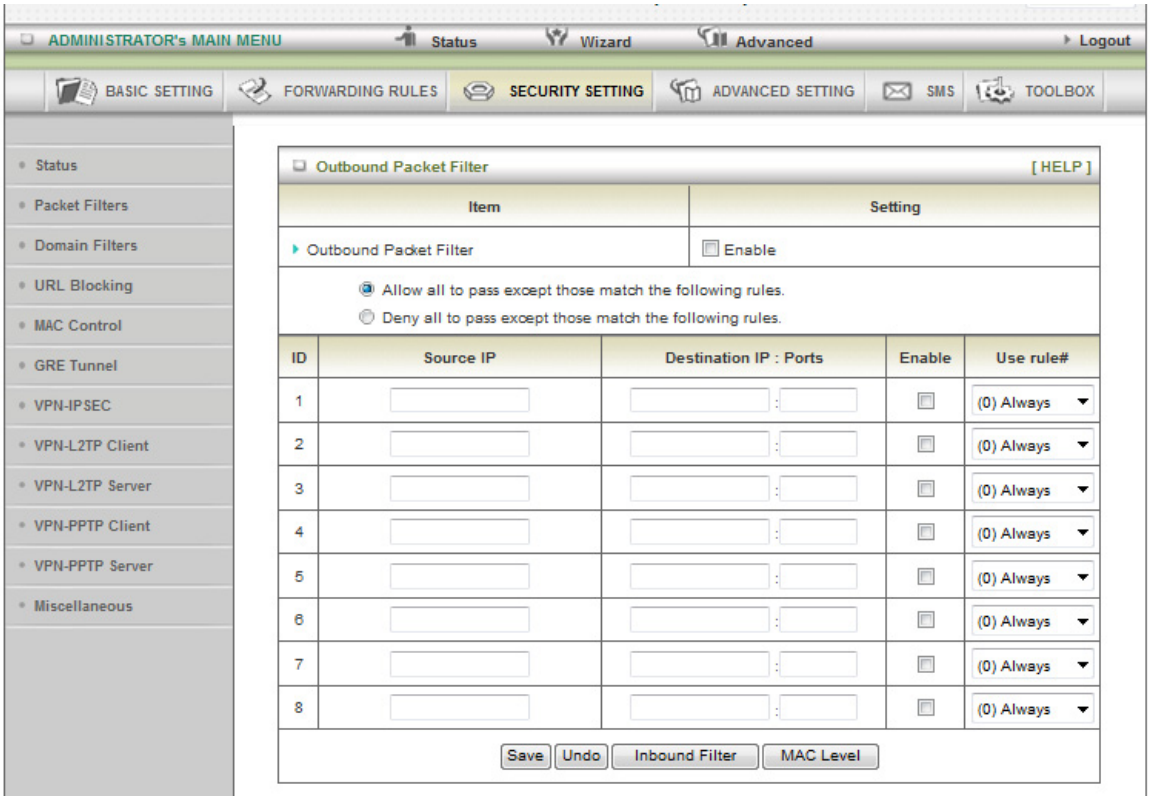
1. **IP Address of DMZ Host**
   DMZ (Demilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.
2. **UPnP Setting**
   The device also supports this function. If the OS supports this function enable it, like Windows XP. When the user gets IP from Device and will see icon as below:

Click on "Save" to store your setting or "Undo" to give up

3.2.3 Security Setting


ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
SMS
TOOLBOX
Status
Packet Filters
Domain Filters
URL Blocking
MAC Control
GRE Tunnel
VPN-IPSEC
VPN-L2TP Client
VPN-L2TP Server
VPN-PPTP Client
VPN-PPTP Server
Miscellaneous
SECURITY SETTING
Packet Filters
- Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
Domain Filters
- Let you prevent users under this device from accessing specific URLs.
URL Blocking
- URL Blocking will block LAN computers to connect to pre-defined websites.
MAC Address Control
- MAC Address Control allows you to assign different access right fordifferent users and to assign a specific IP address to a certain MAC address.
VPN
- VPN Settings are used to create virtual private tunnels to remote VPN gateways.
VPN-L2TP Client
- In order to create virtual private connection via tunneling to remote VPN-L2TP servers.
VPN-L2TP Server
- Provide virtual private connection via tunneling from remote VPN-L2TP clients.
VPN-PPTP Client
- In order to create virtual private connection via tunneling to remote VPN-PPTP servers.
VPN-PPTP Server
- Provide virtual private connection via tunneling from remote VPN-PPTP clients.
Miscellaneous
- Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
- Administrator Time-out: The amount of time of inactivity before the devicewill automatically close the Administrator session. Set this to zero to disable it.
- Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

1. Packet Filters



Packet Filter includes both outbound filter and inbound filter. And they have same way to setting. Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Rule#

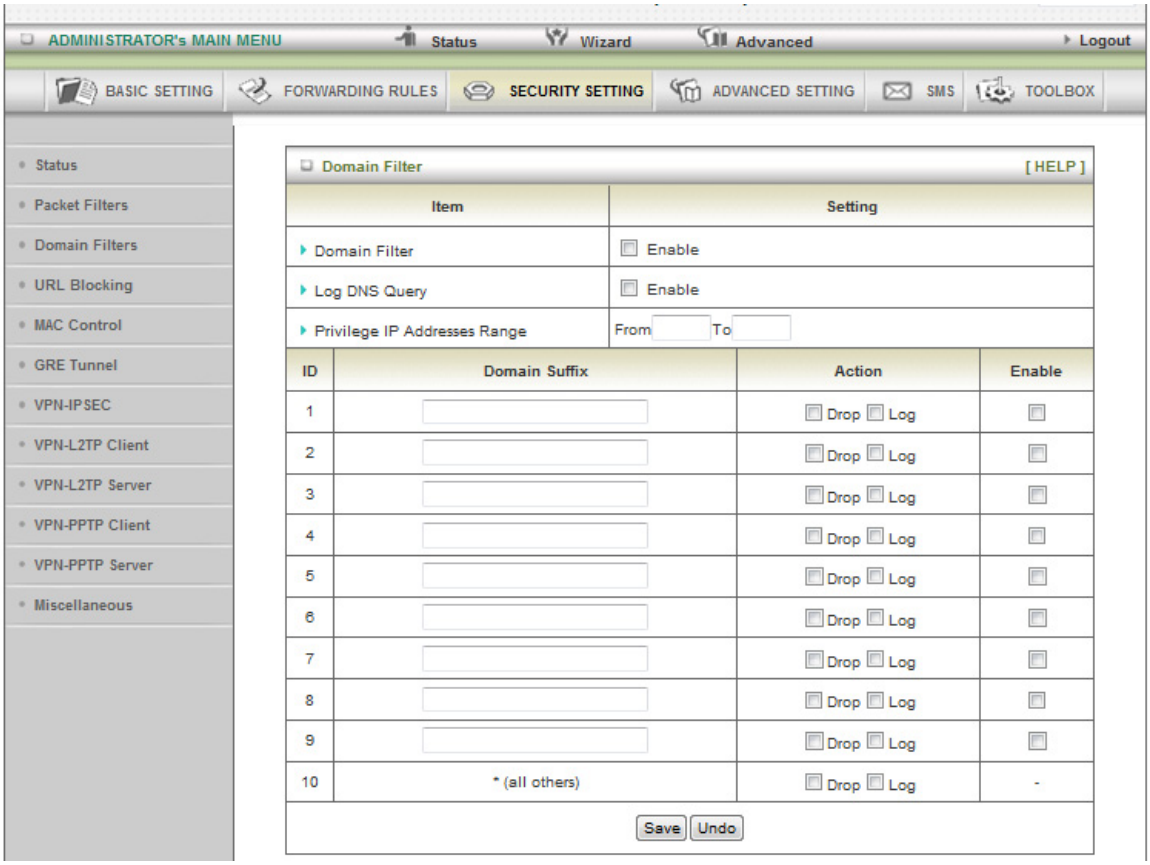
For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with **Scheduling Rules,** and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule.**

Each rule can be enabled or disabled individually.

Click on "Save" to store your setting or "Undo" to give up

2. Domain Filters



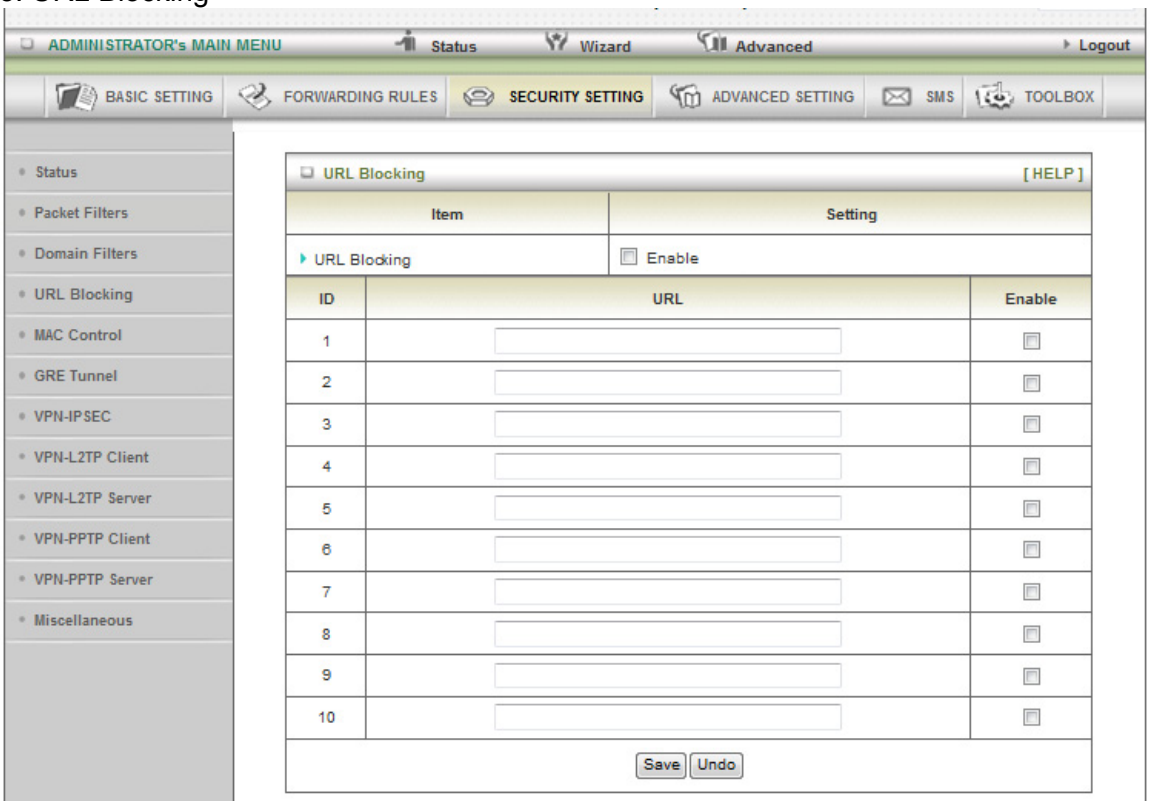
1. **Domain Filter**
   Let you prevent users under this device from accessing specific URLs.
2. **Domain Filter Enable**
   Check if you want to enable Domain Filter.
3. **Log DNS Query**
   Check if you want to log the action when someone accesses the specific URLs.
4. **Privilege IP Address Range**
   Setting a group of hosts and privilege these hosts to access network without restriction.
5. **Domain Suffix**
   A suffix of URL can be restricted, for example, ".com", "xxx.com".
6. **Action**

When someone is accessing the URL met the domain-suffix, what kind of action you want. Check drop to block the access. Check “log” to log these access.

7. **Enable**
   Check to enable each rule.

Click on “Save” to store your setting or “Undo” to give up

3. URL Blocking



URL Blocking will block LAN computers to connect with pre-define Websites. The major difference between “Domain filter” and “URL Blocking” is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a **keyword**.

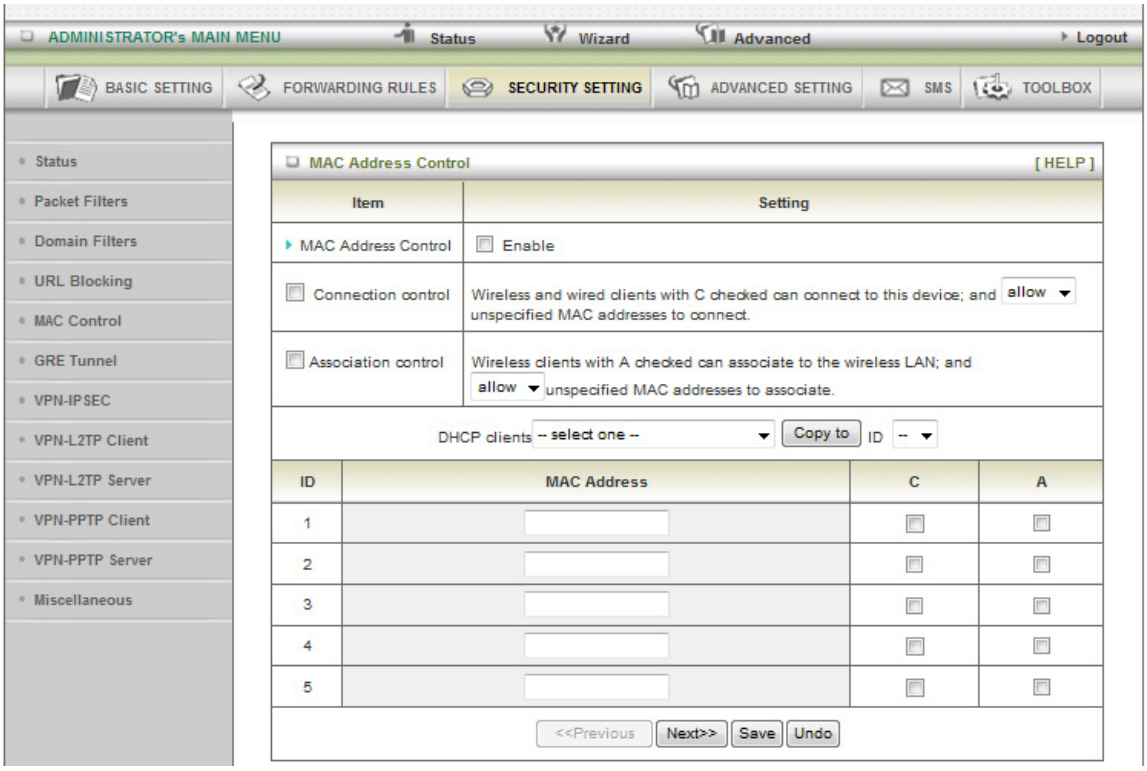
1. **URL Blocking Enable**
   Check if you want to enable URL Blocking.
2. **URL**
   If any part of the Website's URL matches the pre-defined word, the connection will be blocked.
   For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

3. **Enable**

   Check to enable each rule.

   Click on “Save” to store your setting or “Undo” to give up

4. MAC Control



MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

1. **MAC Address Control**

   Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.

2. **Connection control**

   Check "Connection control" to enable the controlling of which wired and wireless clients can connect with this device. If a client is denied to connect with this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect with this device.

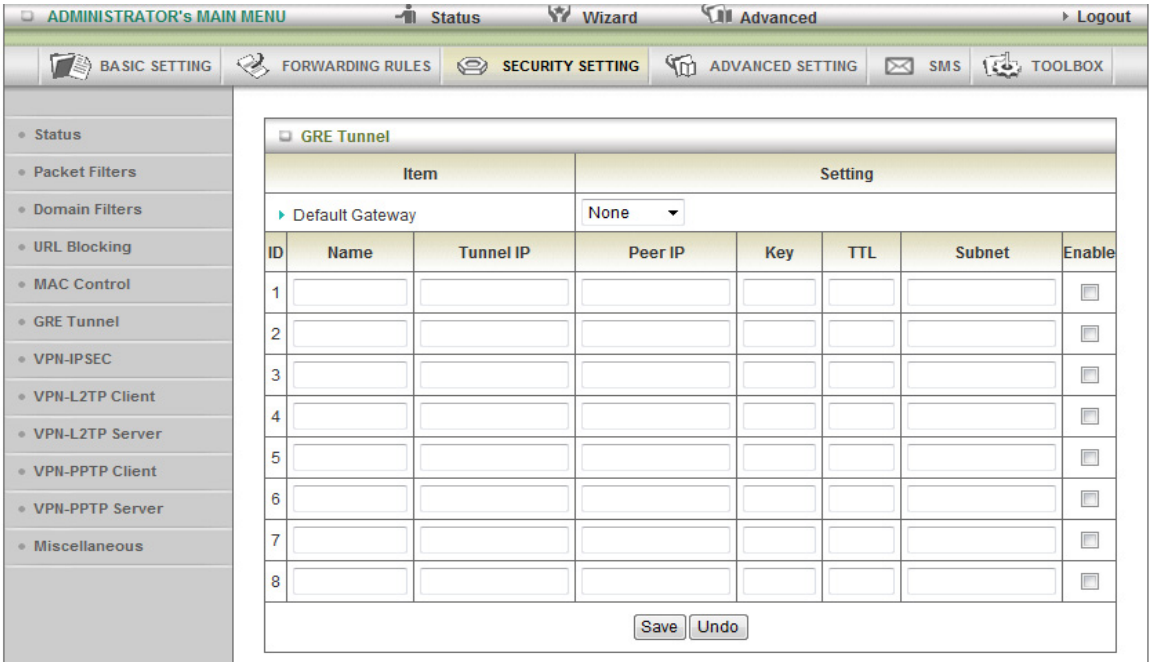
3. **Association control**

   Check "Association control" to enable the controlling of which wireless client can associate

to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN

Click “Save” to store your setting or “Undo” to give up

5. GRE Tunnel



GRE Tunnel allows you to establish GRE tunnel with remote host.

1. **Default Gateway**
   You can choose a tunnel as default gateway for WAN connection, but it doesn’t cover those subnet which exist in other activated GRE tunnel.
2. **Name**
   Assign a name of certain tunnel.
3. **Tunnel IP**
   Assign a virtual IP address of this tunnel.
4. **Peer IP**
   Indicate IP address of remote host that you want to connect.
5. **Key**
   Assign a password to establish GRE tunnel with remote host.
6. **TTL**

Time-To-Live for packets. The value is between 1 to 255. If a packet passes number of TTL routers and can't reach the destination, and then this packet will be dropped.

7. **Subnet**

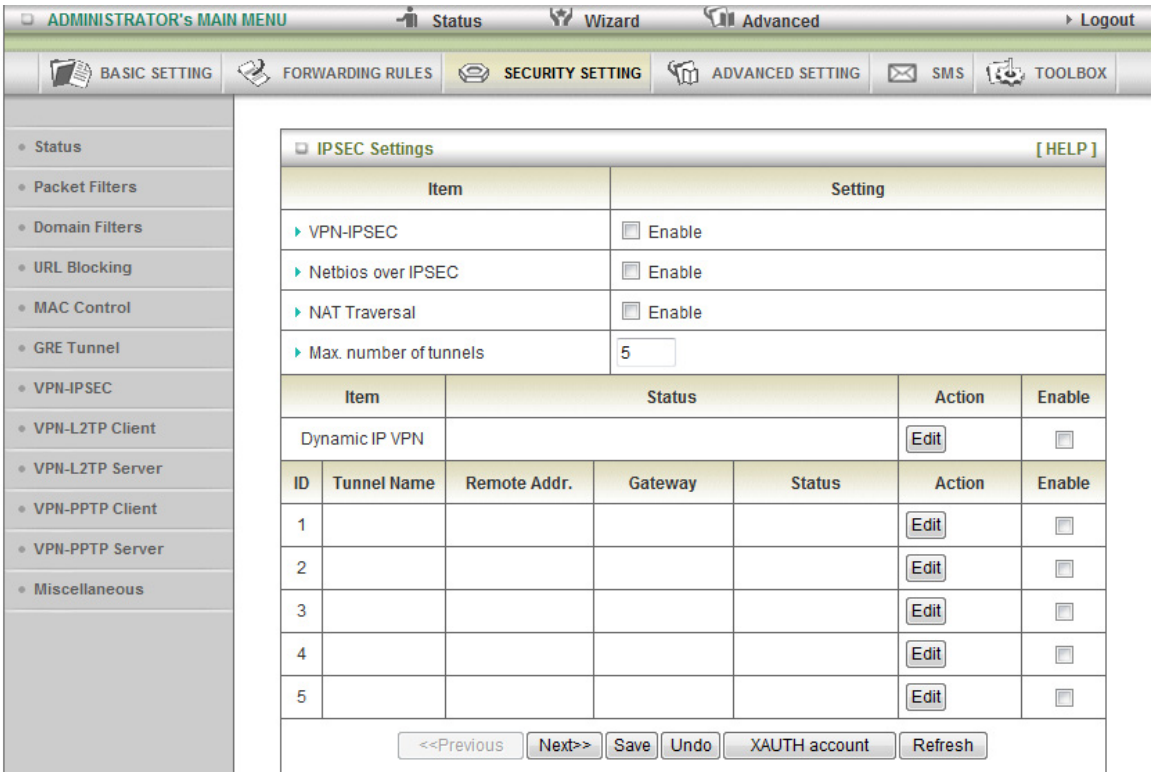
   Indicate local subnet of remote host. If a packet wants to go this subnet, the GRE tunnel will be established automatically.

8. **Enable**

   Check this box to activate this rule.

Click "Save" to store your setting or "Undo" to give up

6. VPN-IPSEC



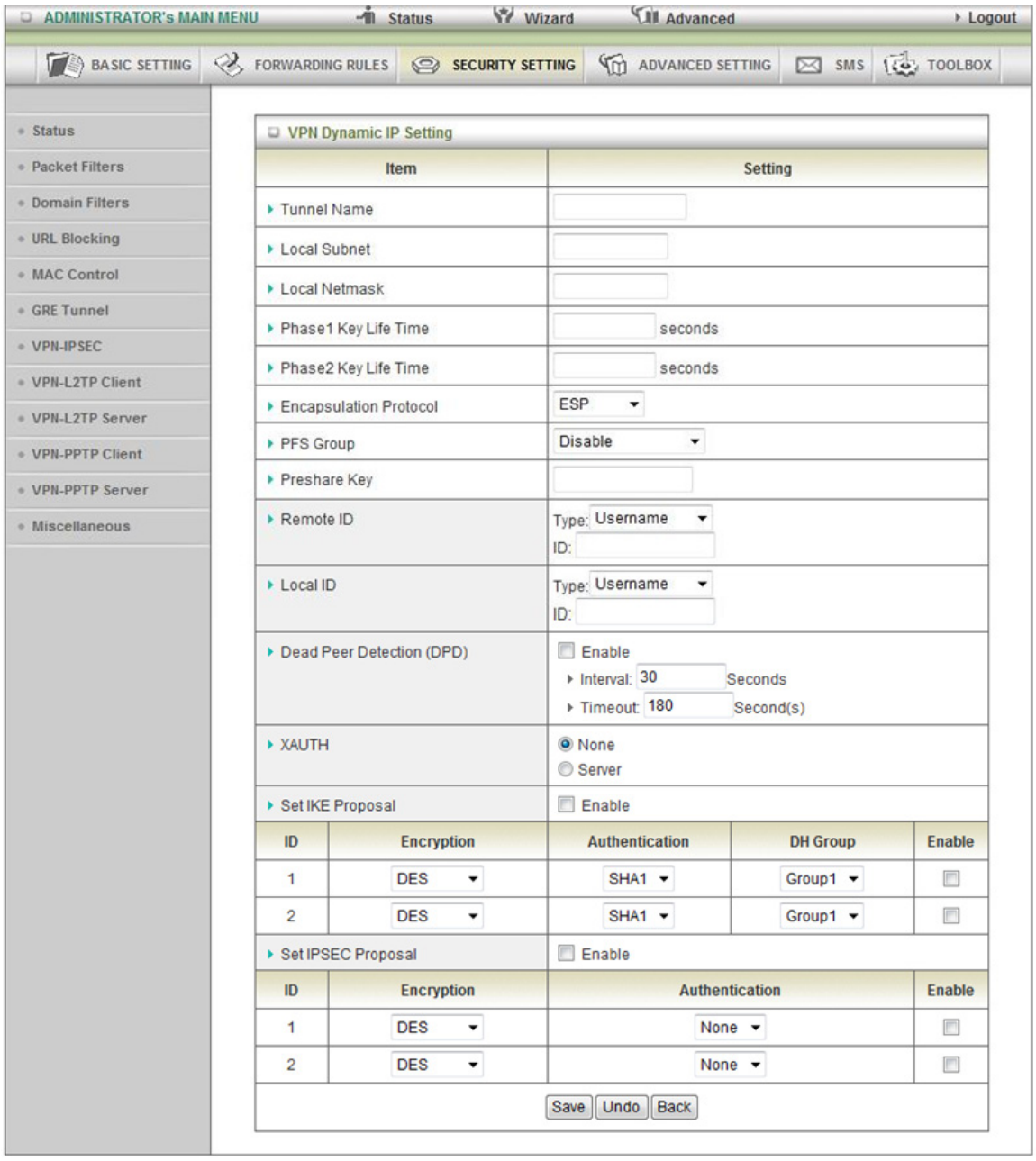
VPN-IPSec are settings that are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

1. **VPN-IPSEC**
   VPN protects network information from ill network inspectors. But it greatly degrades network throughput. Enable it when you really need a security tunnel. It is disabled by default.
2. **Netbios over IPSEC**
   Computers running Microsoft Windows can communicate with one another using NetBIOS. Users can access remote network resources by browsing the Window Network Neighborhood.

3. **NAT Traversal**
   Some NAT router will block IPSec packets if it doesn't support IPSec pass-through. If you connect to another NAT router which doesn't support IPSec pass-through at WAN side, you need to activate this option.
4. **Max. number of tunnels**
   Since VPN greatly degrades network throughput, the allowable maximum number of tunnels is limited. Be careful to set the value for allowing the number of tunnels can be created simultaneously. Its value ranges from 1 to 5.
5. **Dynamic IP VPN**
   Enable it when you need remote mobile hosts build security tunnel with the Gateway. It is disabled by default. Click "Edit" button to finish configuration.
6. **Tunnel Name**
   Name for certain tunnel. Click "Edit" button to finish configuration.

Click on "Save" to store what you just select or" Undo" to give up

6.1 Dynamic IP VPN



VPN gateway can ignore IP information of client when using Dynamic VPN, so it is suitable for users to build VPN tunnel with VPN gateway from remote mobile host.

Tunnel name: Assign a name of this tunnel.

Local subnet: The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, and the whole subnet of LAN site of local gateway.

Local Netmask: Local netmask combined with local subnet to form a subnet domain.
Phase 1 Key Life Time: The unit of life time is based on the value of Life Time Unit. The value of unit is second, the value of life time represents the life time of the key which is dedicated at Phase

1 between both end gateways.

Phase 2 Key Life Time: The unit of life time is based on the value of Life Time Unit. The value of unit is second, the value of life time represents the life time of the key which is dedicated at Phase 2 between both end gateways.

Encapsulation Protocol: There are three protocols can be selected: ESP, AH, or ESP+AH.

PFS Group: Configures Perfect Forward Secrecy for connections created with this IPSec transport profile by assigning a Diffie-Hellman prime modulus group. There are three groups can be selected: Group 1, Group 2, Group 5.

Disable: No PFS group
Group 1: 768-bit Diffie-Hellman prime modulus group
Group 2: 1024-bit Diffie-Hellman prime modulus group
Group 5: 1536-bit Diffie-Hellman prime modulus group

Preshare key: The first key that supports IKE mechanism of both VPN gateway and VPN client host for negotiating further security keys. The pre-shared key must be same for both VPN gateways and clients.

Remote ID: The Type and the Value are must same as the Type and the Value of the Local ID of the remote VPN gateway.

Local ID: The Type and the Value are must same as the Type and the Value of the Remote ID of the remote VPN gateway.

Dead Peer Detection: This feature will detect if remote VPN gateway still exists. Indicate time of interval between every detection, and assigns value of timeout.

XAUTH: With xAuth feature, the VPN client (or initiator) needs to provide additional user information to remote VPN server (or VPN gateway) for extended authentication. The VPN server would reject the connect request from VPN clients because of the unknown user, even though the pre-shared key is correct. This function is suitable to remote mobile VPN clients. You can not only configure a VPN rule with a pre-shared key for all remote users using, but you can also designate only someone is permitted to establish VPN connection with VPN server.
XAUTH - None: Without Extended Authentication(xAuth).
XAUTH -Server: Check this checkbox if the device behaves as a VPN server, and will verify the legality of user information from VPN client. The user information that is provided by VPN client needs to match to user information that is in local user database of VPN server. You can press "XAUTH Account" button at IPSec Setting main page to edit local user database. Please note that only VPN clients with XAUTH can establish VPN connection with the device if you have activated XAUTH function.

Set IKE Proposal: Check this checkbox to enable IKE proposals.

Encryption: There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256.

Authentication: There are two algorithms can be selected: SHA1 and MD5.

DH Group: There are three groups can be selected: Group 1 (MODP768), Group 2 (MODP1024), and Group 5 (MODP1536).

Enable: Check this checkbox to enable the IKE Proposal with this rule.
Set IPSec Proposal: Check this checkbox to enable IPSec proposals.

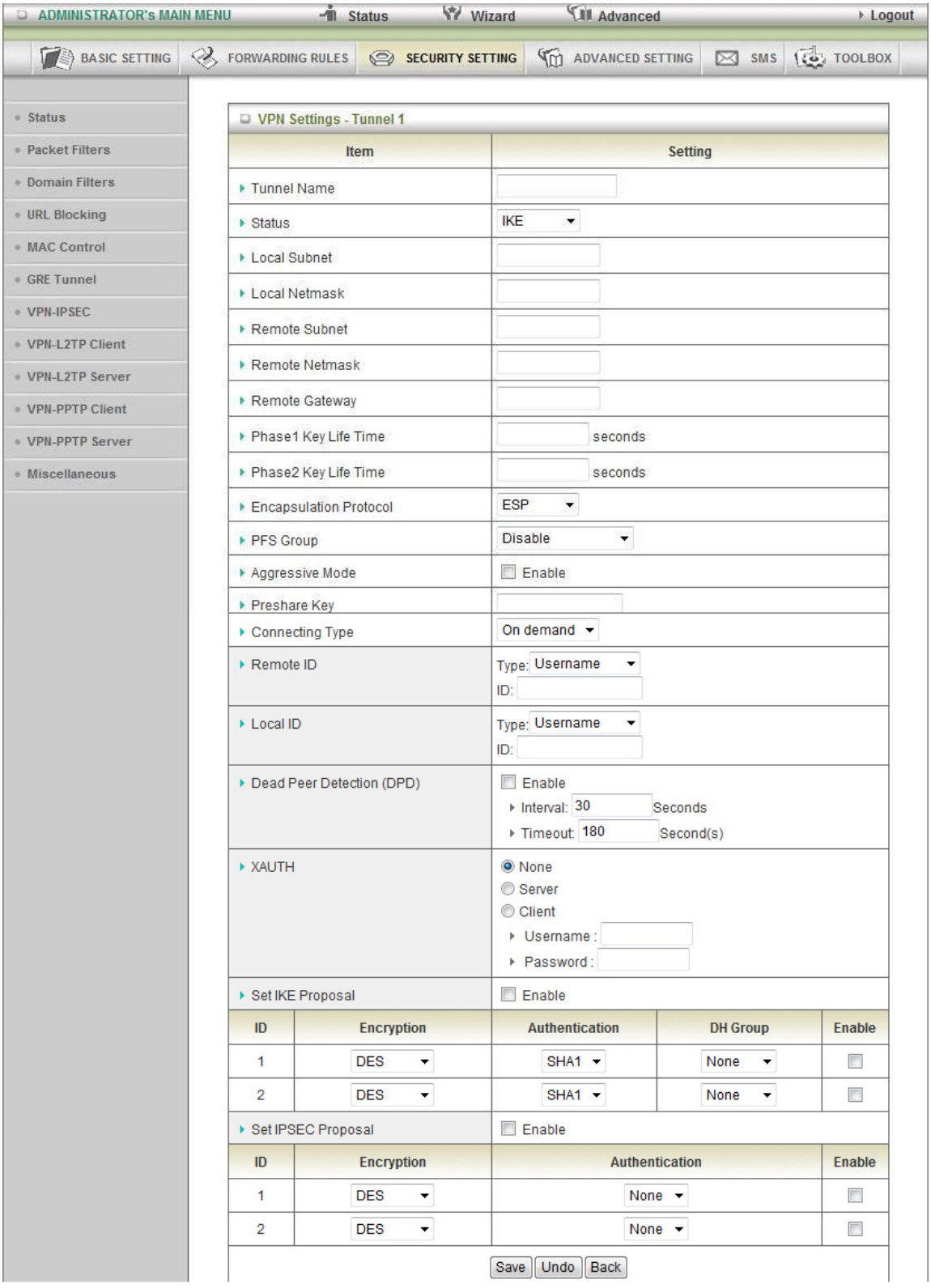
Encryption: There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256. But when the encapsulation protocol is set to AH, you can choose Null without encryption.

Authentication: There are two algorithms can be selected: SHA1 and MD5. But none also can be selected here for IPSec proposal.

Enable: Check this checkbox to enable IPSec Proposal with this rule.

Click on “Save” to store what you just select or” Undo” to give up

6.2 IPSec-IKE Setting



Tunnel name: Assign a name of this tunnel.

Status: There are IKE and Manual two options. Please choose IKE here.

Local subnet: The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, and the whole subnet of LAN site of local gateway.

Local Netmask: Local netmask combined with local subnet to form a subnet domain.

Remote subnet: The subnet of LAN site of remote VPN gateway. It can be a host, a partial subnet, and the whole subnet of LAN site of remote gateway.

Remote Netmask: Remote netmask combined with remote subnet to form a subnet domain.

Remote Gateway: Indicate the IP address of remote VPN gateway.

Phase 1 Key Life Time: The unit of life time is based on the value of Life Time Unit. The value of unit is second, the value of life time represents the life time of the key which is dedicated at Phase 1 between both end gateways.

Phase 2 Key Life Time: The unit of life time is based on the value of Life Time Unit. The value of unit is second, the value of life time represents the life time of the key which is dedicated at Phase 2 between both end gateways.

Encapsulation Protocol: There are three protocols can be selected: ESP, AH, or ESP+AH.

PFS Group: Configures Perfect Forward Secrecy for connections created with this IPSec transport profile by assigning a Diffie-Hellman prime modulus group. There are three groups can be selected: Group 1, Group 2, Group 5.

Disable: No PFS group
Group 1: 768-bit Diffie-Hellman prime modulus group
Group 2: 1024-bit Diffie-Hellman prime modulus group
Group 5: 1536-bit Diffie-Hellman prime modulus group

Aggressive Mode: Enabling this mode will accelerate establishing tunnel, but the device will suffer from less security in the meanwhile. Hosts in both ends of the tunnel must support this mode so as to establish the tunnel properly.

Preshare key: The first key that supports IKE mechanism of both VPN gateway and VPN client host for negotiating further security keys. The pre-shared key must be same for both VPN gateways and clients.

Connecting Type: There are three options for users to choose when the VPN tunnel will be established. You can choose connect on-demand, always connect, or connect manually.

Remote ID: The Type and the Value are must same as the Type and the Value of the Local ID of the remote VPN gateway.

Local ID: The Type and the Value are must same as the Type and the Value of the Remote ID of the remote VPN gateway.

Dead Peer Detection: This feature will detect if remote VPN gateway still exists. Indicate time of interval between every detection, and assigns value of timeout.

XAUTH: With xAuth feature, the VPN client (or initiator) needs to provide additional user information to remote VPN server (or VPN gateway) for extended authentication. The VPN server would reject the connect request from VPN clients because of the unknown user, even though the pre-shared key is correct. This function is suitable to remote mobile VPN clients. You can not only configure a VPN rule with a pre-shared key for all remote users using, but you can also designate

only someone is permitted to establish VPN connection with VPN server.
XAUTH - None: Without Extended Authentication(xAuth).
XAUTH -Server: Check this checkbox if the device behaves as a VPN server, and will verify the legality of user information from VPN client. The user information that is provided by VPN client needs to match to user information that is in local user database of VPN server. You can press "XAUTH Account" button at IPSec Setting main page to edit local user database. Please note that only VPN clients with XAUTH can establish VPN connection with the device if you have activated XAUTH function.
XAUTH -Client: Check this checkbox if the device behaves as a VPN server, and will send user information to remote VPN server for extended authentication. You need to input correct user name and password to pass authentication. Please note that remote VPN server which is without xAuth will reject your connect request if you have checked this checkbox.

Set IKE Proposal: Check this checkbox to enable IKE proposals.

Encryption: There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256.

Authentication: There are two algorithms can be selected: SHA1 and MD5.

DH Group: There are three groups can be selected: Group 1 (MODP768), Group 2 (MODP1024), and Group 5 (MODP1536).

Enable: Check this checkbox to enable the IKE Proposal with this rule.

Set IPSec Proposal: Check this checkbox to enable IPSec proposals.

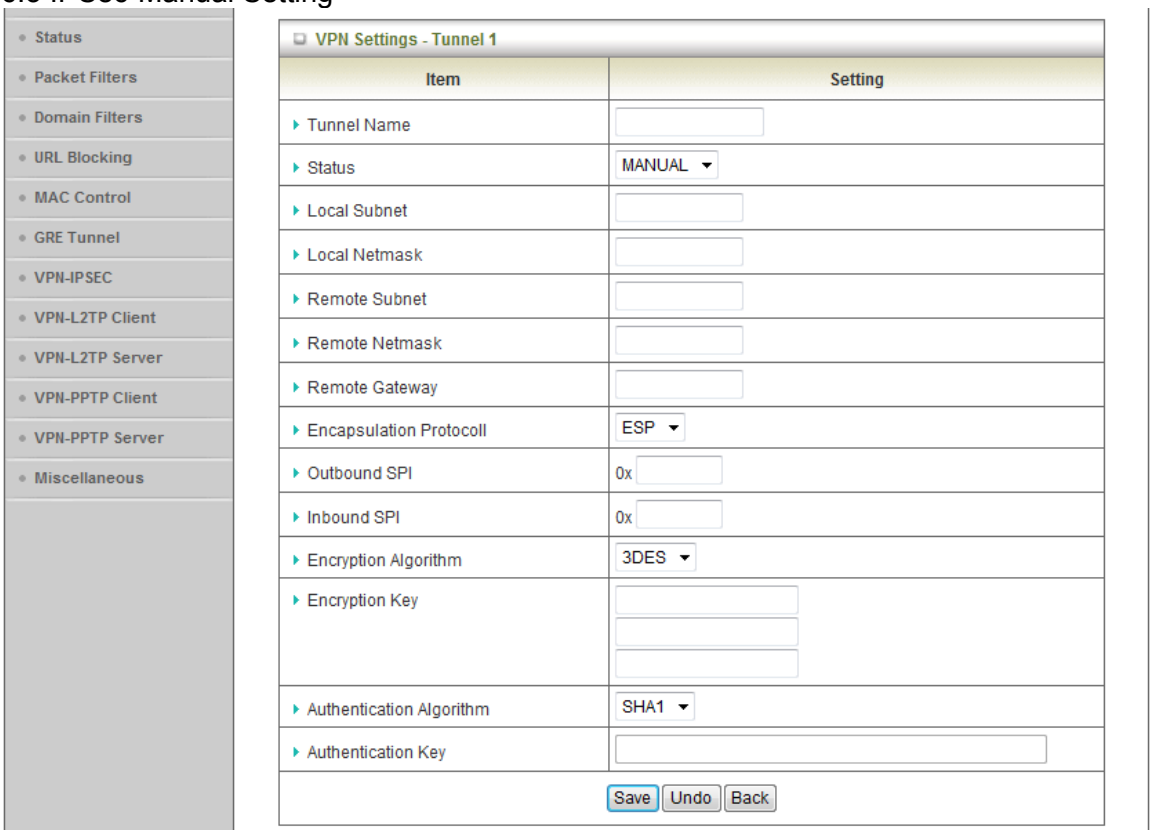
Encryption: There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256. But when the encapsulation protocol is set to AH, you can choose Null without encryption.

Authentication: There are two algorithms can be selected: SHA1 and MD5. But none also can be selected here for IPSec proposal.

Enable: Check this checkbox to enable IPSec Proposal with this rule.

Click on “Save” to store what you just select or” Undo” to give up

6.3 IPSec-Manual Setting



Tunnel name: Assign a name of this tunnel.

Status: There are IKE and Manual two options. Please choose Manual here.

Local subnet: The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, and the whole subnet of LAN site of local gateway.

Local Netmask: Local netmask combined with local subnet to form a subnet domain.

Remote subnet: The subnet of LAN site of remote VPN gateway. It can be a host, a partial subnet, and the whole subnet of LAN site of remote gateway.

Remote Netmask: Remote netmask combined with remote subnet to form a subnet domain.

Remote Gateway: Indicate the IP address of remote VPN gateway.

Encapsulation Protocol: There are two protocols can be selected: ESP or AH.

Outbound SPI: SPI is an important parameter during hashing. Outbound SPI will be included in the outbound packet transmitted from local gateway. The value of outbound SPI should be set in hex formatted.

Inbound SPI: Inbound SPI will be included in the inbound packet transmitted from WAN site of remote gateway. It will be used to de-hash the coming packet and check its integrity. The value of outbound SPI should be set in hex formatted.

Encryption: There are two algorithms can be selected: DES, 3DES.

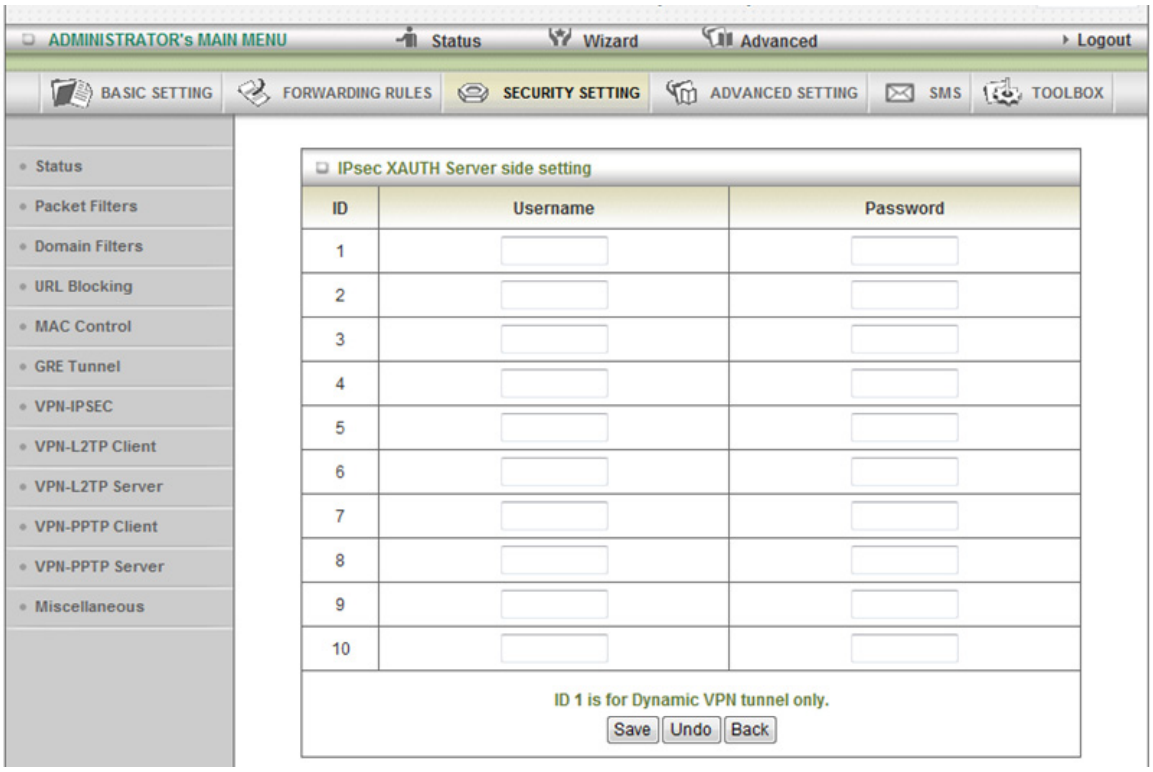
Encryption Key: Encryption key is used by the encryption algorithm. Its length is 8 bytes if encryption algorithm is DES or 24 bytes if 3DES. The key value should be set in hex formatted.

Authentication Algorithm: There are two algorithms can be selected: SHA1 and MD5.

Authentication Key: Authentication key is used by the authentication algorithm. Its length is 16 bytes if authentication algorithm is MD5 or 20 bytes if SHA1. Certainly, its length will be 0 if no authentication algorithm is chosen. The key value should be set in hex formatted.

Click on "Save" to store what you just select or" Undo" to give up

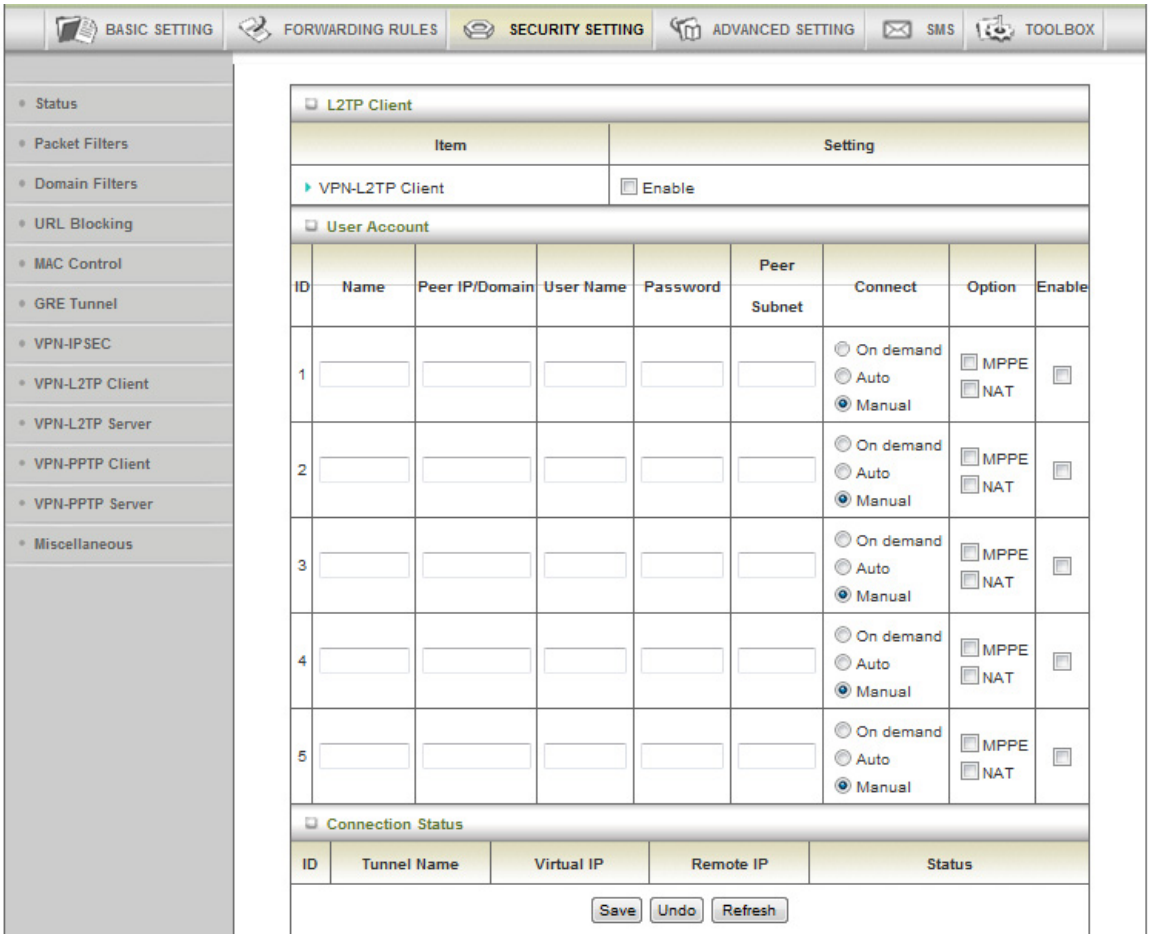
6.4 XAUTH Account



You can edit user information with this configuration page. This user information is for XAuth server mode use only.

Click on "Save" to store what you just select or" Undo" to give up

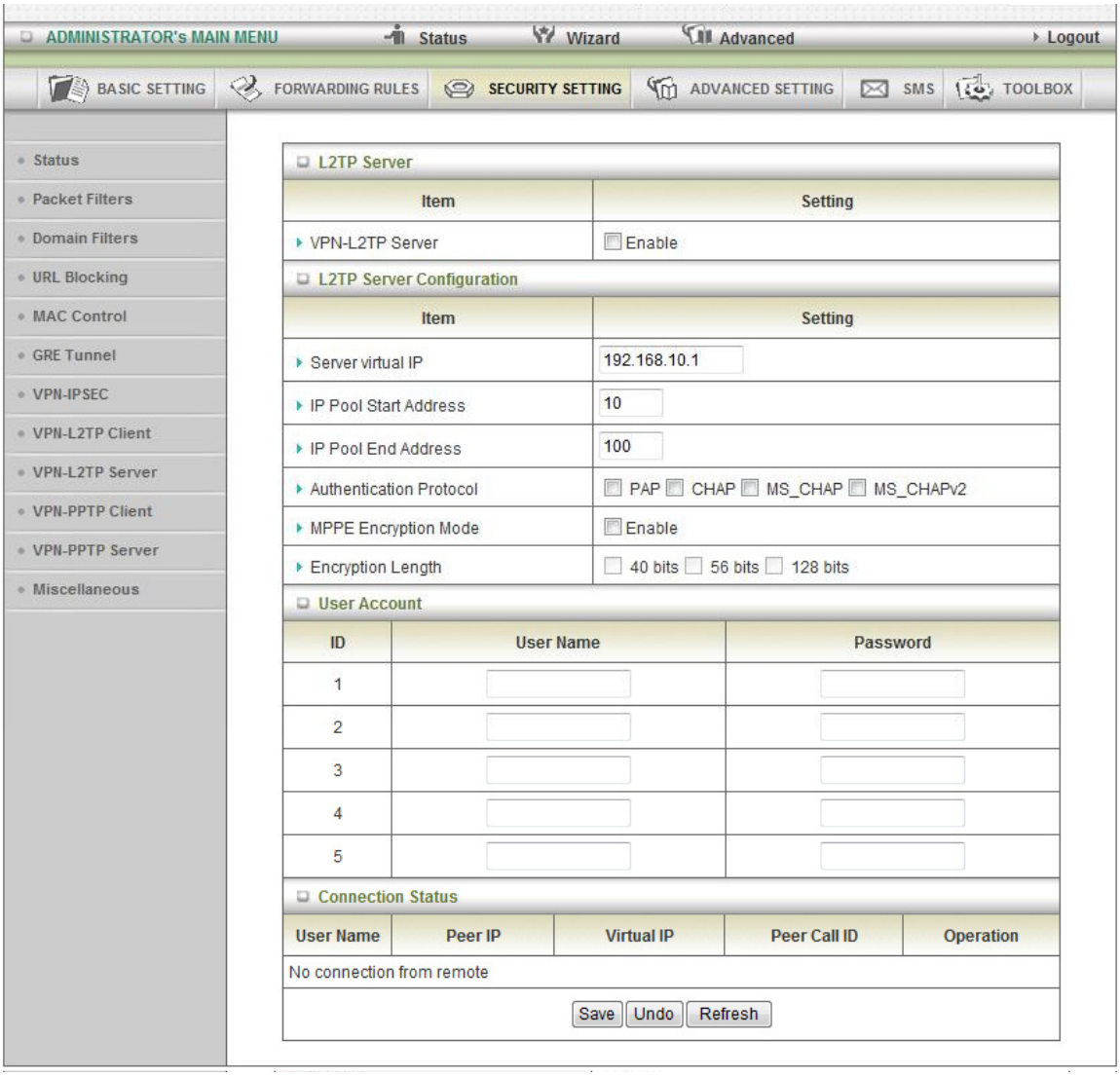
7. VPN L2TP Client



1. **VPN-L2TP Client:** Enable or Disable L2TP client function.
2. **Name:** The name of this rule.
3. **Peer IP/Domain:** The IP address or Domain name of remote L2TP server.
4. **User Name:** The user name which is provided by remote L2TP server.
5. **Password:** The password which is provided by remote L2TP server.
6. **Peer Subnet:** The LAN subnet of remote L2TP server.
7. **Connect:** There are three options for users to choose when the L2TP tunnel will be established. You can choose connect on-demand, Auto(always connect), or connect manually.
8. **Option:** Enable or disable MPPE and NAT function. If you enable MPPE, then this L2TP tunnel will be encrypted.
9. **Enable:** Check to enable this rule.

Click on "Save" to store what you just select or" Undo" to give up

8. VPN L2TP Server



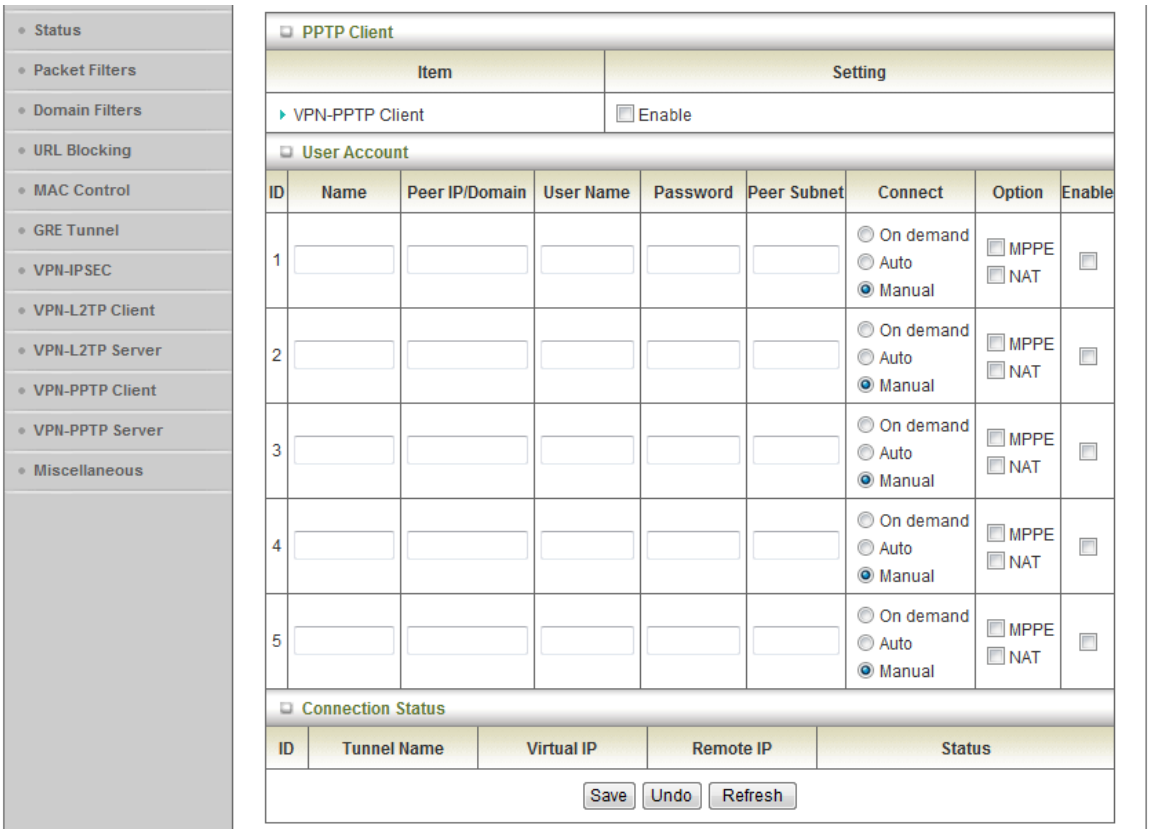
The VPN gateway can behave as a L2TP server, and allows remote hosts to access LAN servers after establishing L2TP connection with it. The device can support three authentication methods: PAP, CHAP, MSCHAP(v1) and MSCHAP(v2). Users can also enable MPPE encryption when using MSCHAP.

1. **VPN-L2TP Server:** Enable or Disable L2TP server function.
2. **Server Virtual IP:** The IP address of L2TP server. This IP address should be different from IP address of PPTP server and LAN subnet of VPN gateway.
3. **IP Pool Start Address:** This device will assign a IP address to remote L2TP client. This values indicates the beginning of IP pool.
4. **IP Pool End Address:** This device will assign a IP address to remote L2TP client. This values indicates the end of IP pool.
5. **Authentication Protocol:** Users can choose authentication protocol as PAP, CHAP, MSCHAP(v1), or MSCHAP(v2).
6. **MPPE Encryption Mode:** Check this checkbox to enable MPPE encryption. Please note that MPPE needs to work with MSCHAP-v1 or MSCHAP-v2 authentication method.

7. **Encryption Length:** You can choose encryption length of MPPE encryption.
8. **User Account:** You can input five different user accounts for L2TP server.
9. **Connection Status:** Here you can see the L2TP connection which has been established.

Click on "Save" to store what you just select or" Undo" to give up

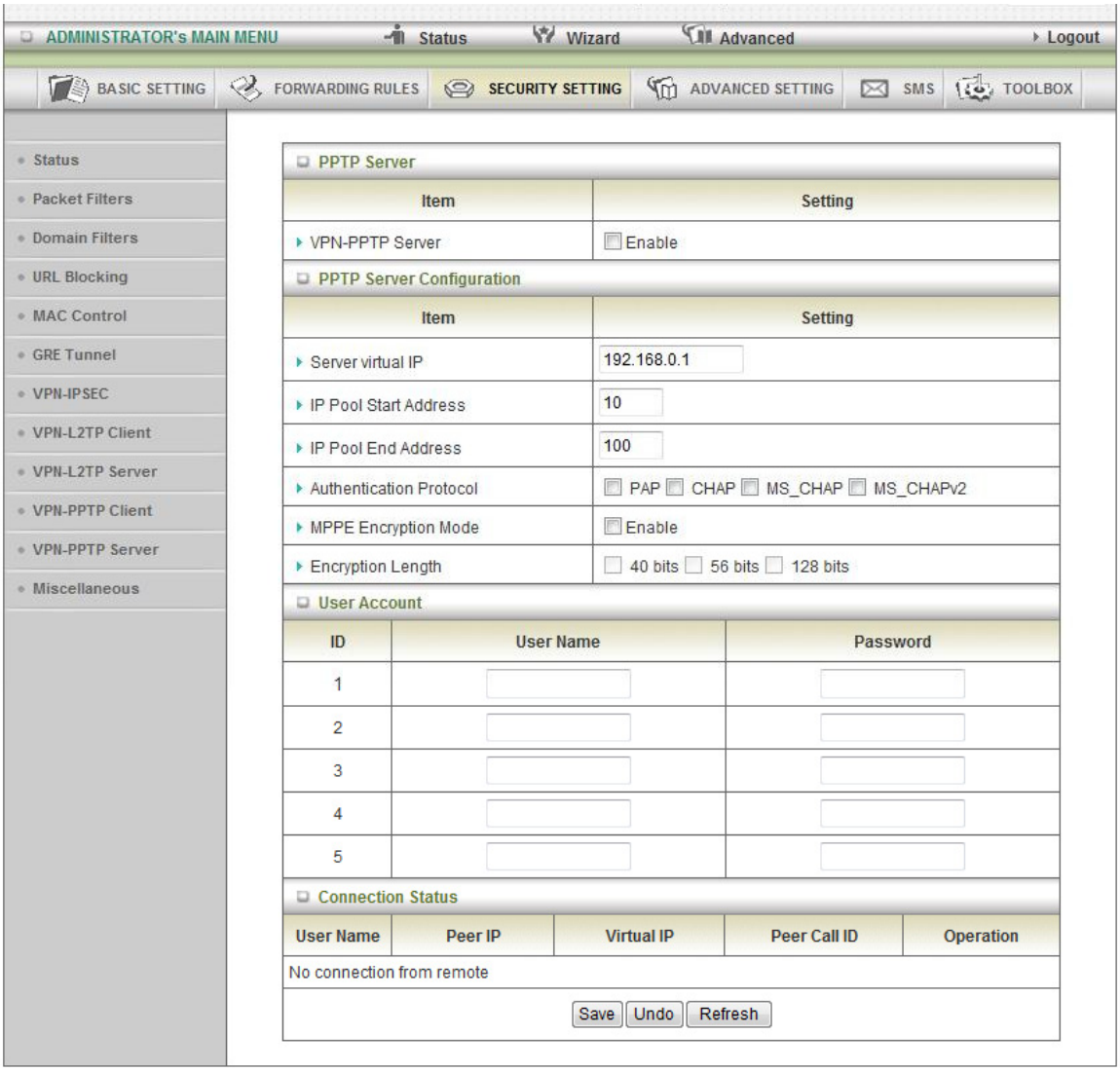
9. VPN PPTP Client



1. **VPN-PPTP Client:** Enable or Disable PPTP client function.
2. **Name:** The name of this rule.
3. **Peer IP/Domain:** The IP address or Domain name of remote PPTP server.
4. **User Name:** The user name which is provided by remote PPTP server.
5. **Password:** The password which is provided by remote PPTP server.
6. **Peer Subnet:** The LAN subnet of remote PPTP server.
7. **Connect:** There are three options for users to choose when the PPTP tunnel will be established. You can choose connect on-demand, Auto(always connect), or connect manually.
8. **Option:** Enable or disable MPPE and NAT function. If you enable MPPE, then this PPTP tunnel will be encrypted.
9. **Enable:** Check to enable this rule.

Click on "Save" to store what you just select or" Undo" to give up

10. VPN PPTP Server



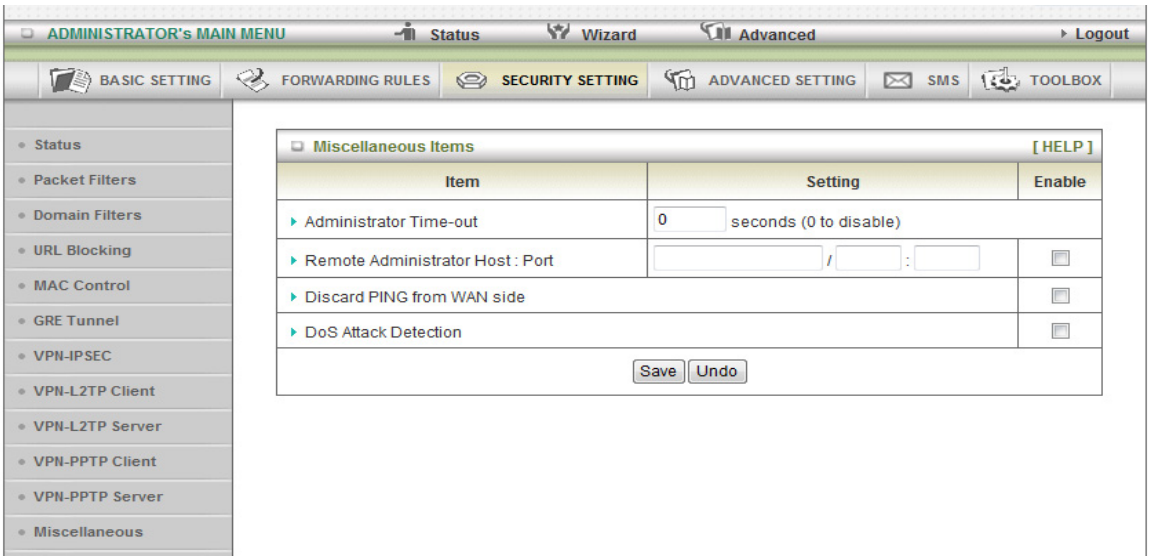
The VPN gateway can behave as a PPTP server, and allows remote hosts to access LAN servers after establishing PPTP connection with it. The device can support three authentication methods: PAP, CHAP, MSCHAP(v1) and MSCHAP(v2). Users can also enable MPPE encryption when using MSCHAP.

1. **VPN-PPTP Server:** Enable or Disable PPTP server function.
2. **Server Virtual IP:** The IP address of PPTP server. This IP address should be different from IP address of L2TP server and LAN subnet of VPN gateway.
3. **IP Pool Start Address:** This device will assign a IP address to remote PPTP client. This values indicates the beginning of IP pool.
4. **IP Pool End Address:** This device will assign a IP address to remote PPTP client. This values indicates the end of IP pool.
5. **Authentication Protocol:** Users can choose authentication protocol as PAP, CHAP, MSCHAP(v1), or MSCHAP(v2).
6. **MPPE Encryption Mode:** Check this checkbox to enable MPPE encryption. Please note that MPPE needs to work with MSCHAP-v1 or MSCHAP-v2 authentication method.
7. **Encryption Length:** You can choose encryption length of MPPE encryption.

8. **User Account:** You can input five different user accounts for PPTP server.
9. **Connection Status:** Here you can see the PPTP connection which has been established.

Click on "Save" to store what you just select or" Undo" to give up

11. Miscellaneous



1. **Administrator Time-out:**
   The time of no activity to logout automatically, you may set it to zero to disable this feature.

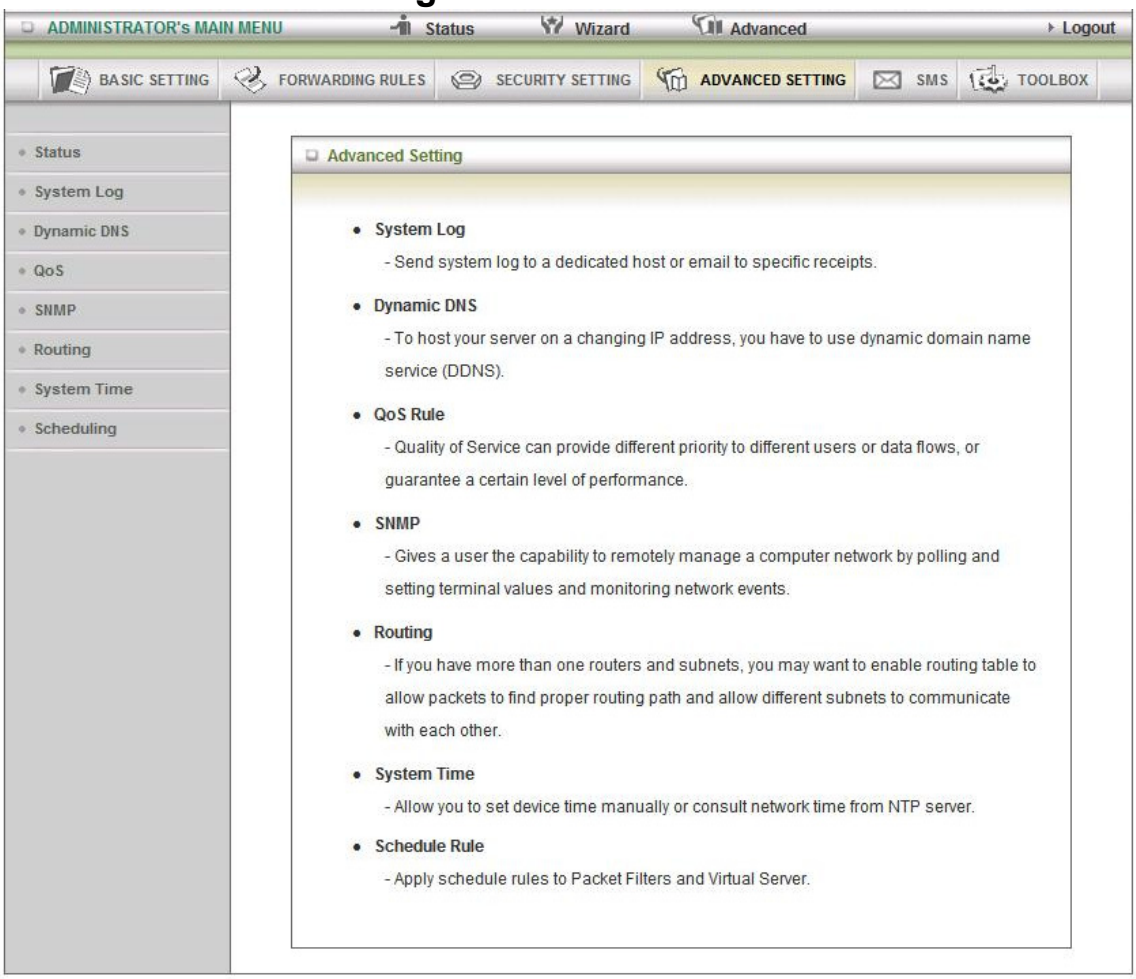
2. **Remote Administrator Host/Port:**
   In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses for example, "10.1.2.0/24".
   NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port, too.

3. **Discard PING from WAN side**
   When this feature is enabled, any host on the WAN cannot ping this product.

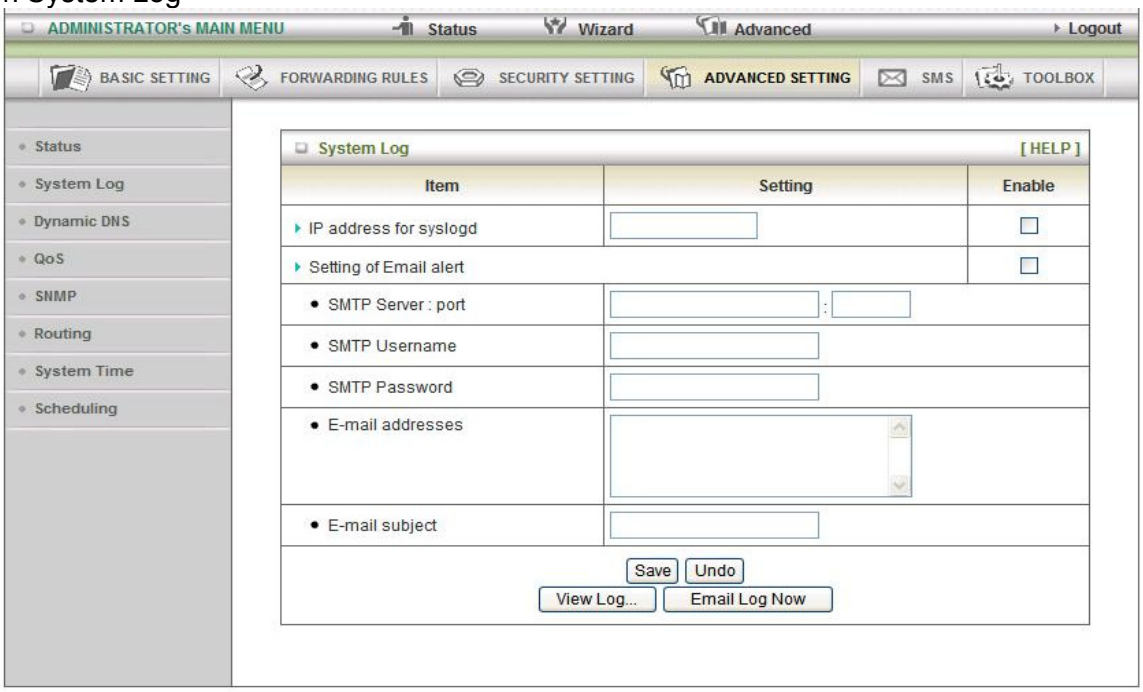
4. **DoS Attack Detection**
   When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

Click on "Save" to store your setting or" Undo" to give up

3.2.4 Advanced Settings


ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
SMS
TOOLBOX
Status
System Log
Dynamic DNS
QoS
SNMP
Routing
System Time
Scheduling
Advanced Setting
System Log
- Send system log to a dedicated host or email to specific receipts.
Dynamic DNS
- To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
QoS Rule
- Quality of Service can provide different priority to different users or data flows, or guarantee a certain level of performance.
SNMP
- Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
Routing
- If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.
System Time
- Allow you to set device time manually or consult network time from NTP server.
Schedule Rule
- Apply schedule rules to Packet Filters and Virtual Server.

1. System Log



This page support two methods to export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). The items you have to setup including:

IP Address for Sys log

Host IP of destination where sys log will be sent to.

Check **Enable** to enable this function.

Setting of E-mail Alert

Check if you want to enable Email alert (send syslog via email).

SMTP Server IP and Port

Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25.

For example, "mail.your_url.com" or "192.168.1.100:26".

SMTP Username and Password

Input a user account and password for the SMTP server.

E-mail address

The recipients who will receive these logs, you can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

E-mail Subject

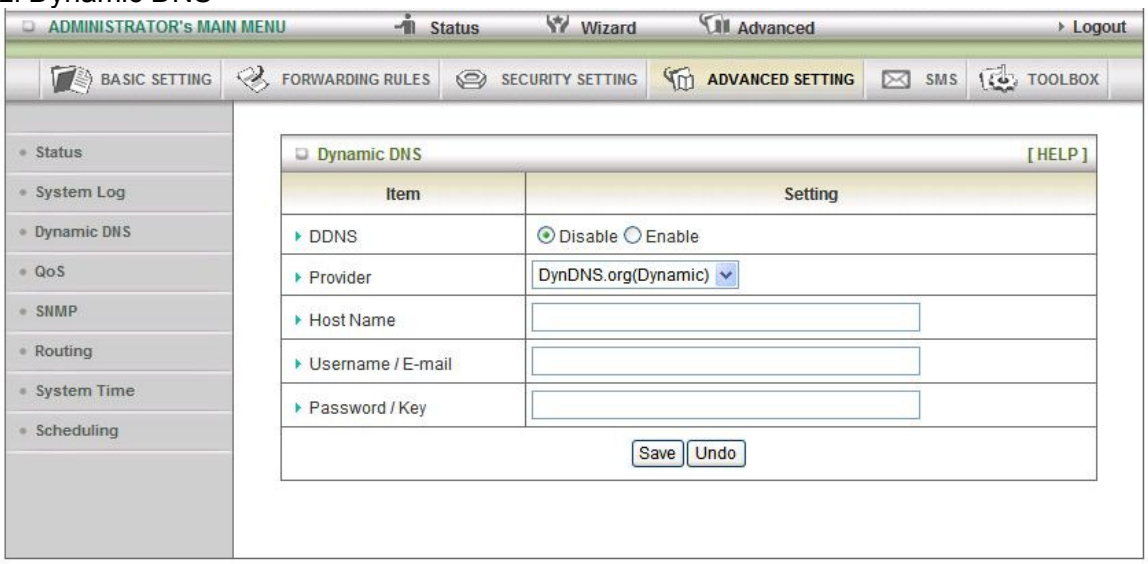
The subject of email alert, this setting is optional.

View Log…

Reference the section Toolbox/System Info.

Click on “Save” to store your setting or “Undo” to give up

2. Dynamic DNS



To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).

So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **provider** field.

To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field.

Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:

Provider

Host Name

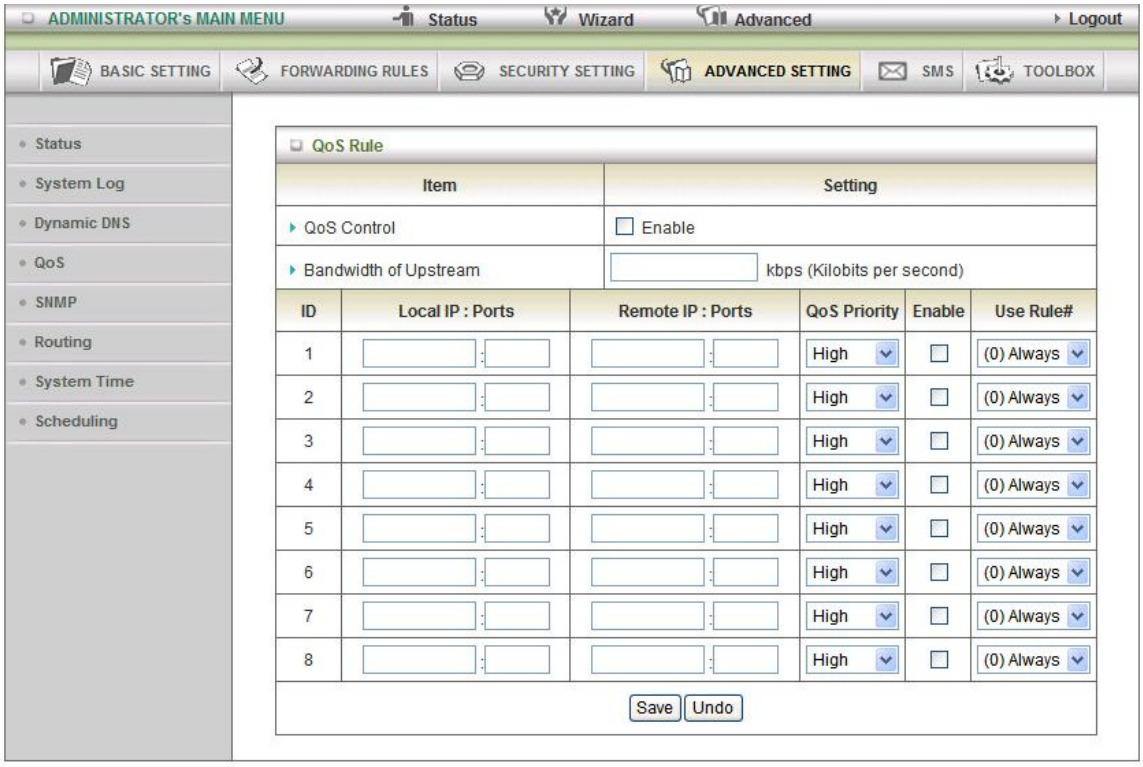
Username/E-mail

Password/Key

You will get this information when you register an account on a Dynamic DNS server.

Click on “Save” to store your setting or “Undo” to give up

3. QoS



Provide different priority to different users or data flows, or guarantee a certain level of performance.

Enable

This Item enables QoS function or not.

Bandwidth of Upstream

Set the limitation of upstream speed.

Local: IP

Define the Local IP address of packets here.

Local: Ports

Define the Local port of the packets in this field.

Remote: IP

Define the Remote IP address of packets here.

Remote: Ports

Define the Remote port of the packets in this field.

QoS Priority

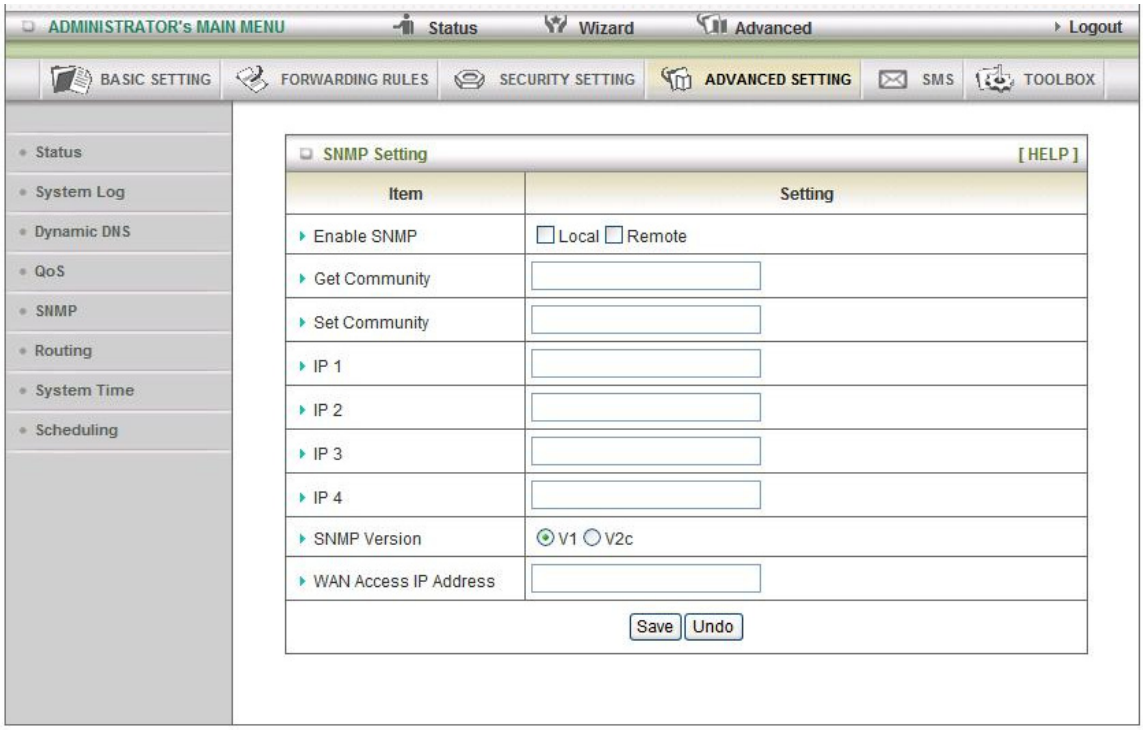
This defines the priority level of the current Policy Configuration. Packets associated with this policy will be serviced based upon the priority level set. For critical applications High or Normal levels are recommended. For non-critical applications select a Low level.

User Rule#

The QoS item can work with Scheduling Rule number#. Please reference the section Advanced setting/schedule Rule.

Click on "Save" to store your setting or "Undo" to give up

4. SNMP



In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

Enable SNMP

You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

Get Community

Setting the community of GetRequest your device will response.

Set Community

Setting the community of SetRequest your device will accept.

IP 1, IP 2, IP 3, IP 4

Input your SNMP Management PC's IP here. User has to configure to where this device should send SNMP Trap message.

SNMP Version

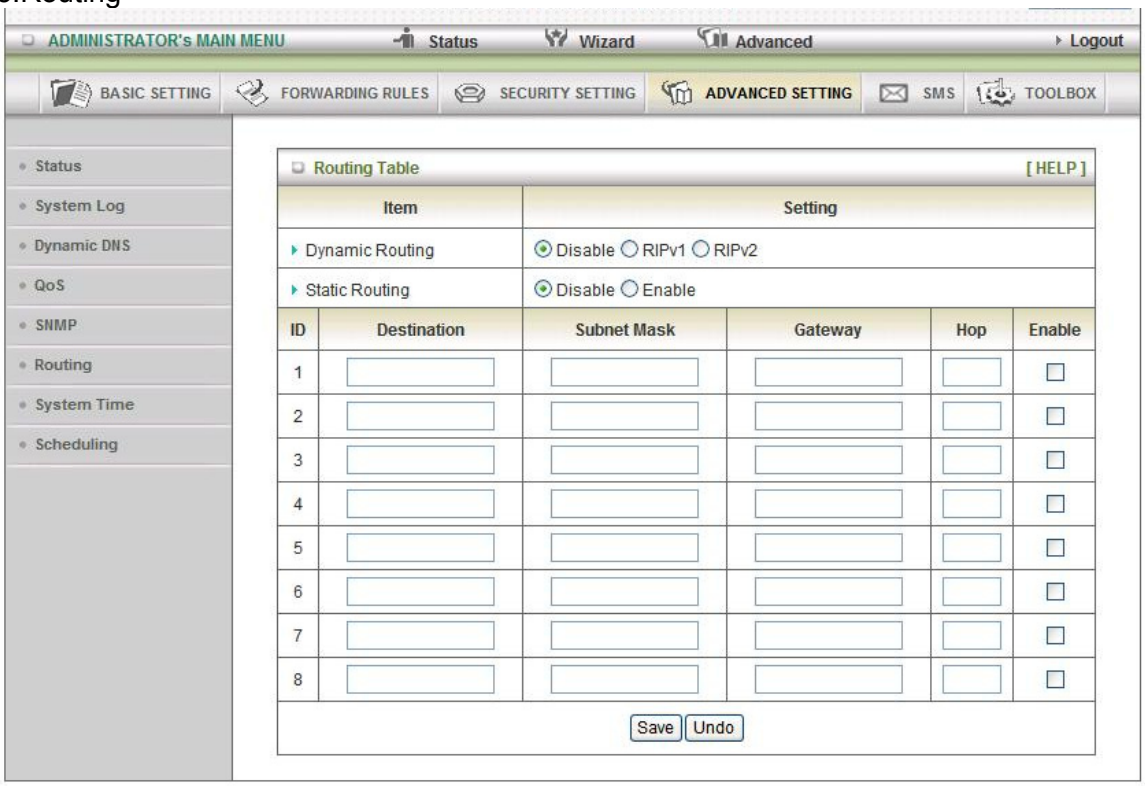
Please select proper SNMP Version that your SNMP Management software supports.

WAN Access IP Address

If the user wants to limit to specific the IP address to access, please input in the item. The default 0.0.0.0 and means every IP of Internet can get some information of device with SNMP protocol.

Click on "Save" to store your setting or "Undo" to give up.

5.Routing



Routing Tables

Allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

Routing Table settings are settings used to setup the functions of static and dynamic routing.

Dynamic Routing

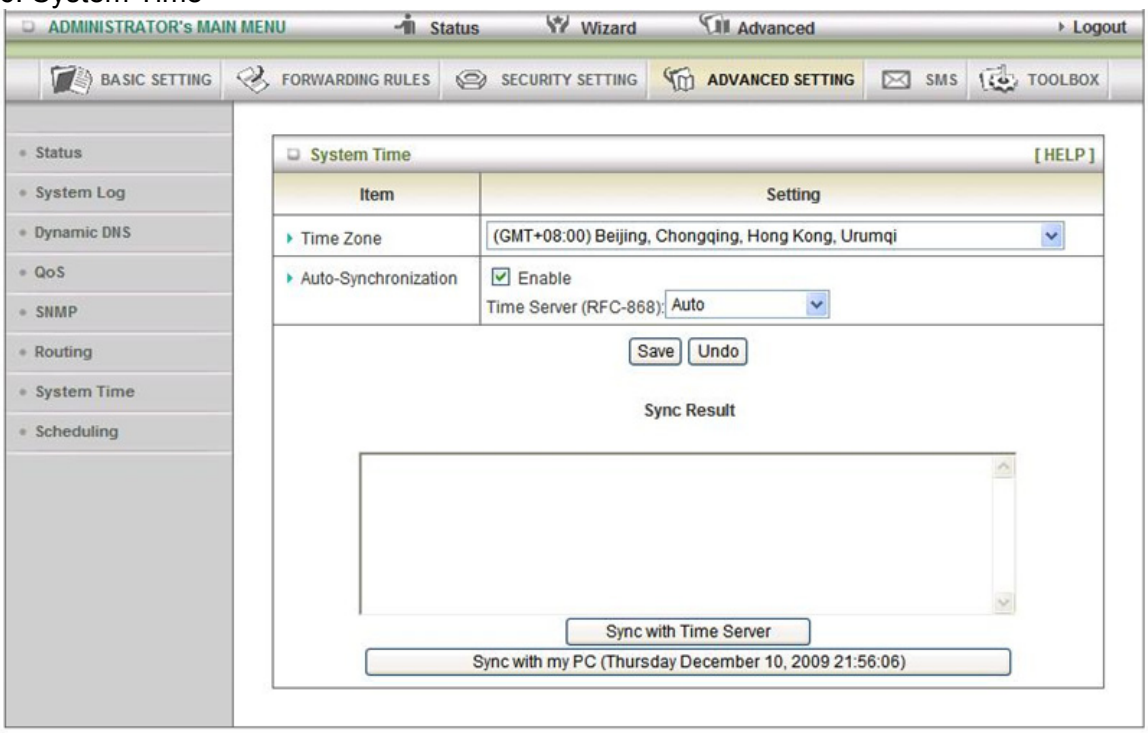
Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

Static Routing

For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, Router, hop for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

Click on “Save” to store your setting or “Undo” to give up.

6. System Time



Time Zone

Select a time zone where this device locates.

Auto-Synchronization

Select the “Enable” item to enable this function.

Time Server

Select a NTP time server to consult UTC time

Sync with Time Server

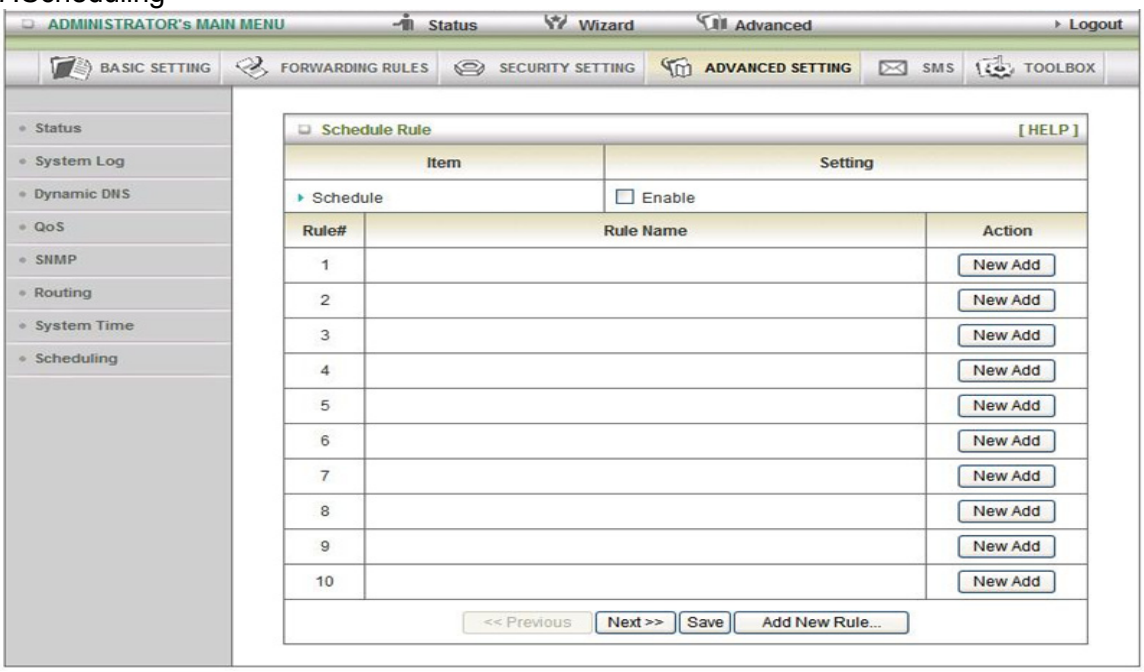
Select if you want to set Date and Time by NTP Protocol.

Sync with my PC

Select if you want to set Date and Time using PC’s Date and Time

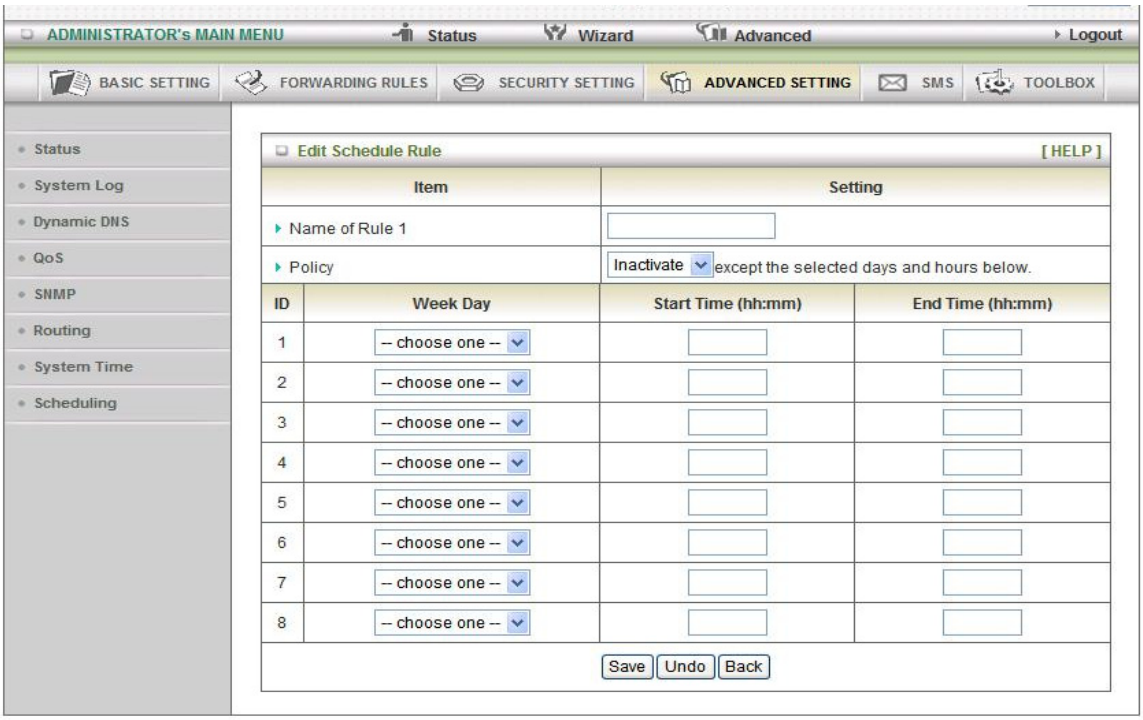
Click on “Save” to store your setting or “Undo” to give up.

7.Scheduling



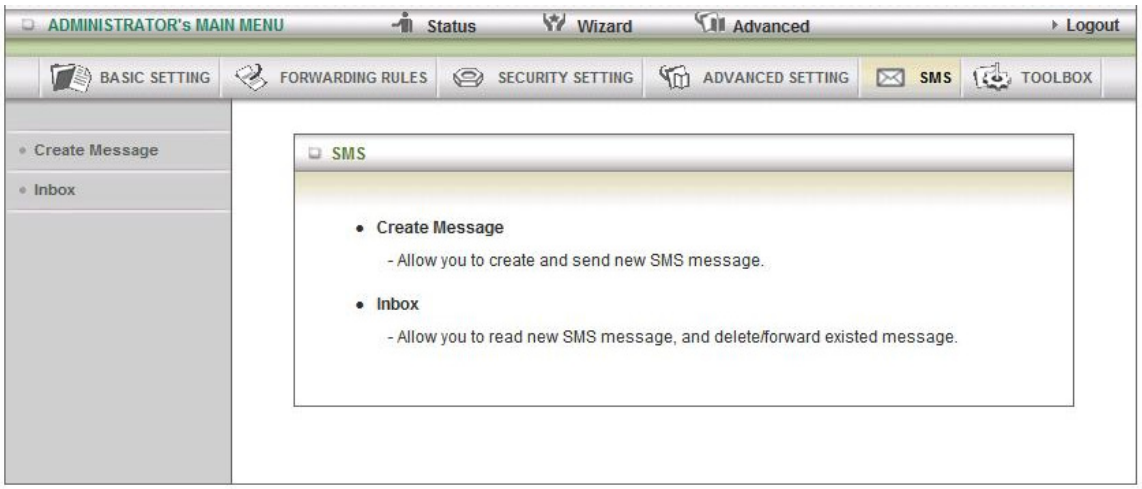
You can set the schedule time to decide which service will be turned on or off.

Select the “Enable” item. Press “Add New Rule” You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”. The following example configure “ftp time” as everyday 14:10 to 16:20

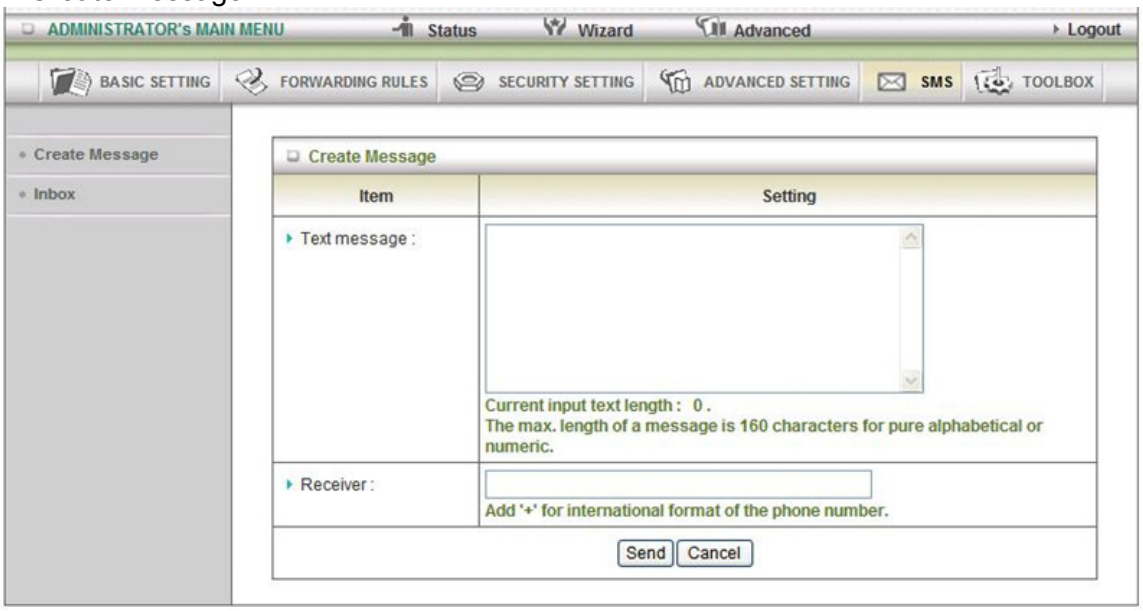


Click on “Save” to store your setting.

3.2.5 SMS

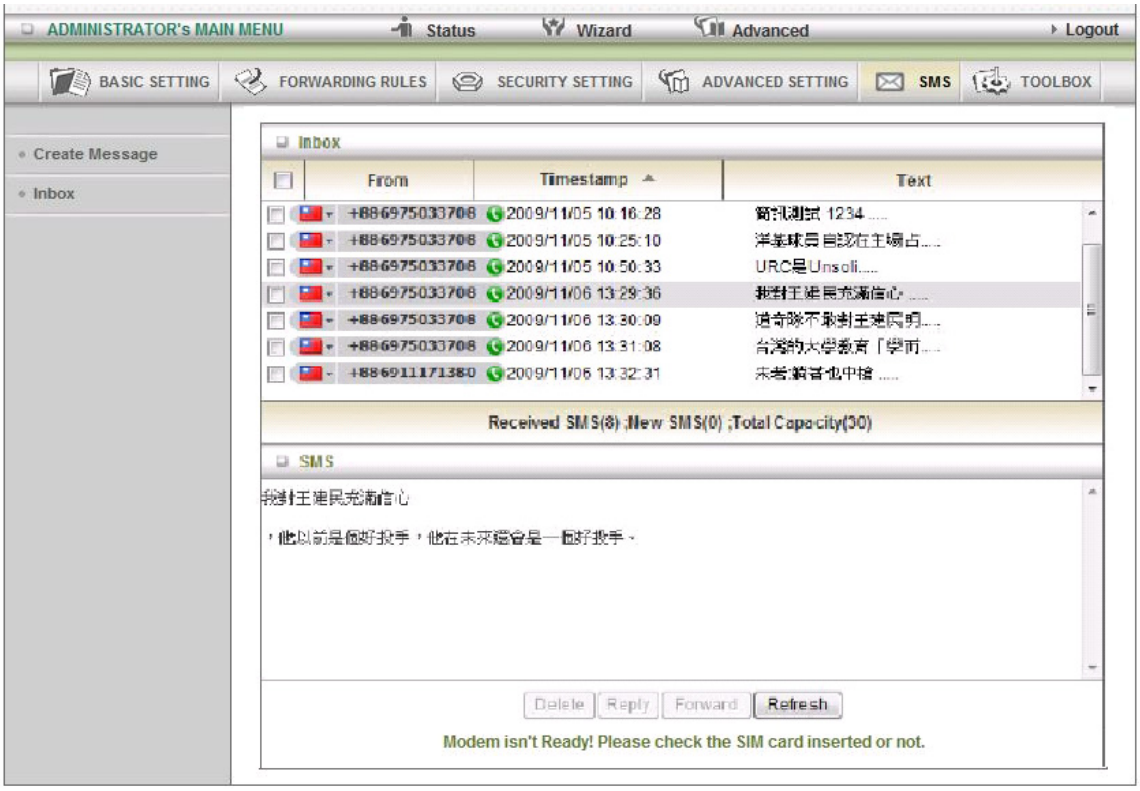


1. Create Message



You can create a new SMS message on this page. After finishing content of message, and filling with phone number of receiver(s), pressing send button to send this message out. You can see “Send OK” if the new message has been sent successfully.

2. Inbox



You can read, delete, reply, and forward messages. Just click on one from the SMS lists, then you can view the whole content of it in the SMS window below.

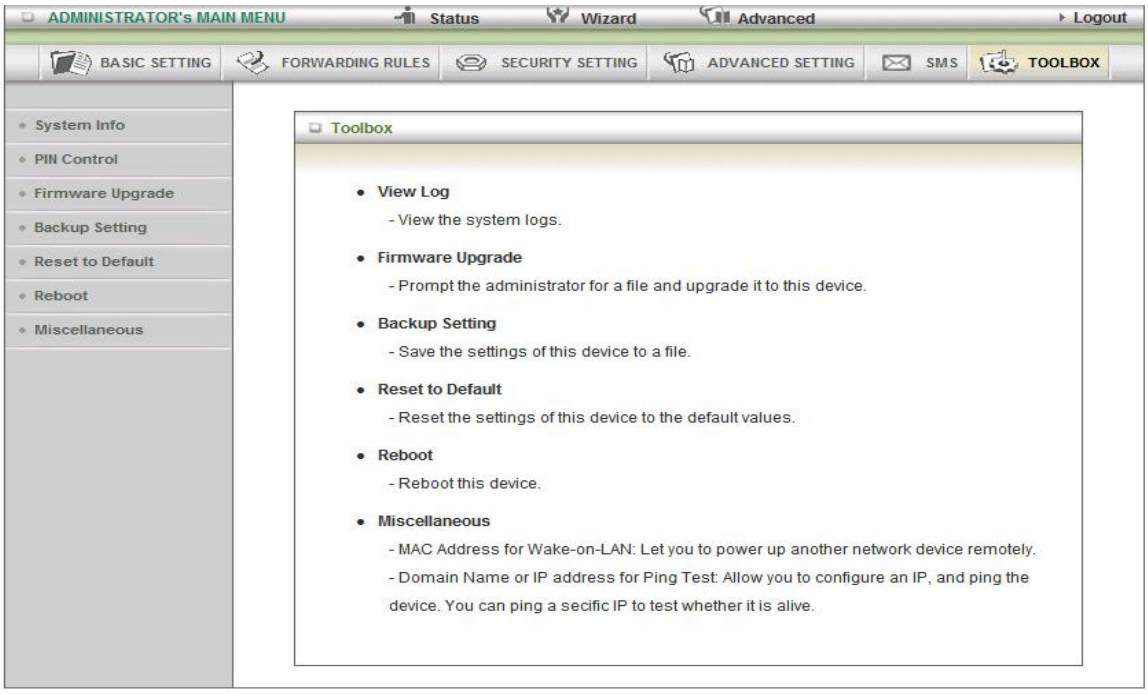
Refresh:

You can press “Refresh” button to renew SMS lists.

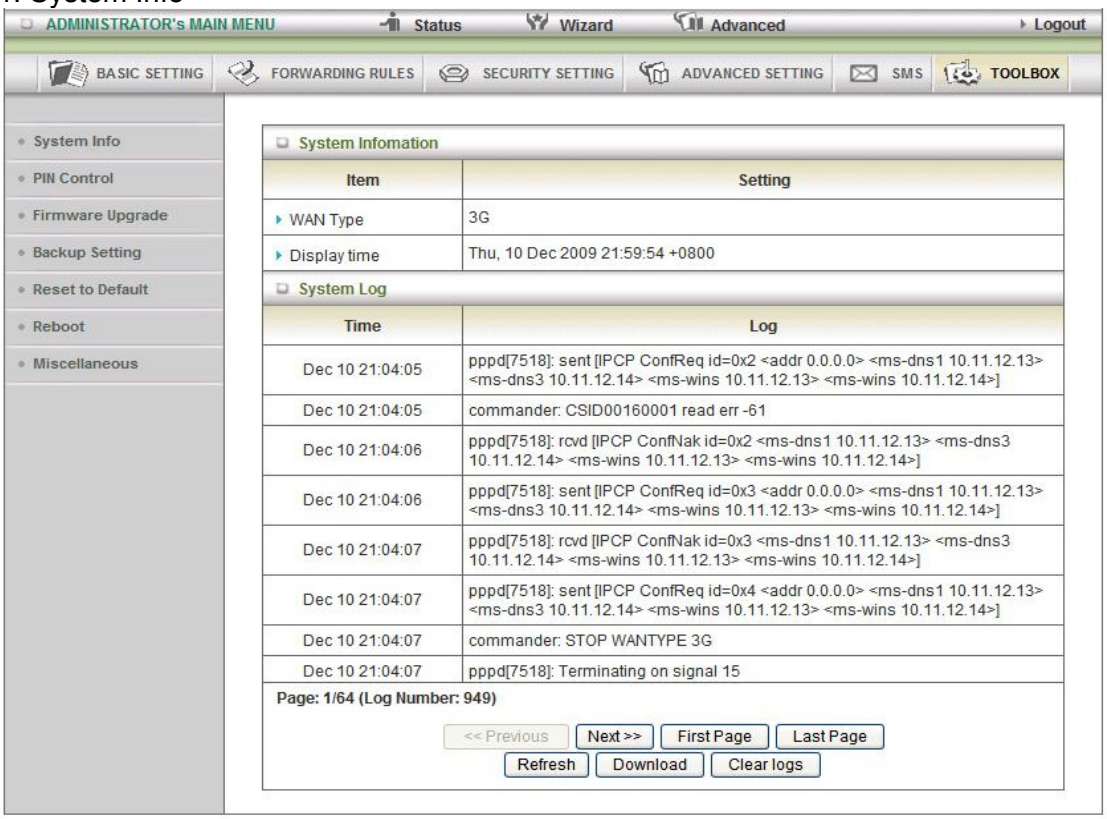
Delete, Reply, Forward Messages:

After reading message, you can check the checkbox on the left of each message to delete, reply, or forward this message.

3.2.6 Tool Box

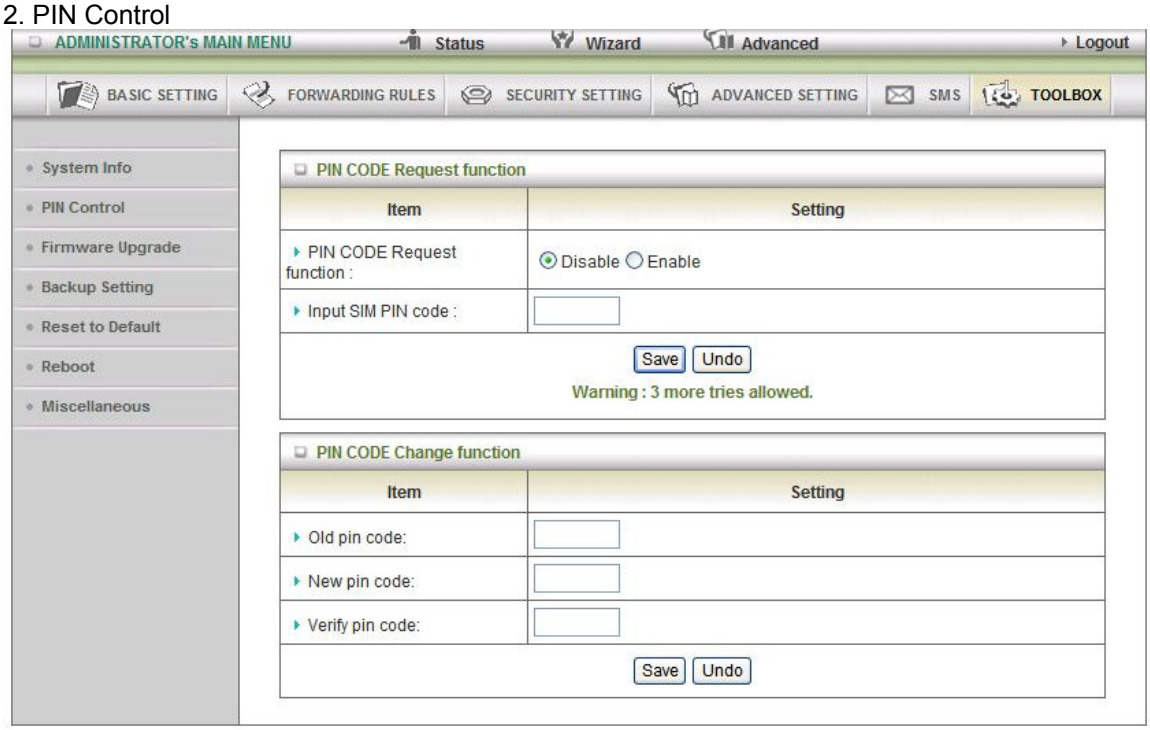

ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
SMS
TOOLBOX
System Info
PIN Control
Firmware Upgrade
Backup Setting
Reset to Default
Reboot
Miscellaneous
Toolbox
View Log
- View the system logs.
Firmware Upgrade
- Prompt the administrator for a file and upgrade it to this device.
Backup Setting
- Save the settings of this device to a file.
Reset to Default
- Reset the settings of this device to the default values.
Reboot
- Reboot this device.
Miscellaneous
- MAC Address for Wake-on-LAN: Let you to power up another network device remotely.
- Domain Name or IP address for Ping Test: Allow you to configure an IP, and ping the device. You can ping a secific IP to test whether it is alive.

1. System Info



You can view the System Information and System log, and download/clear the System log, in this page.

2. PIN Control



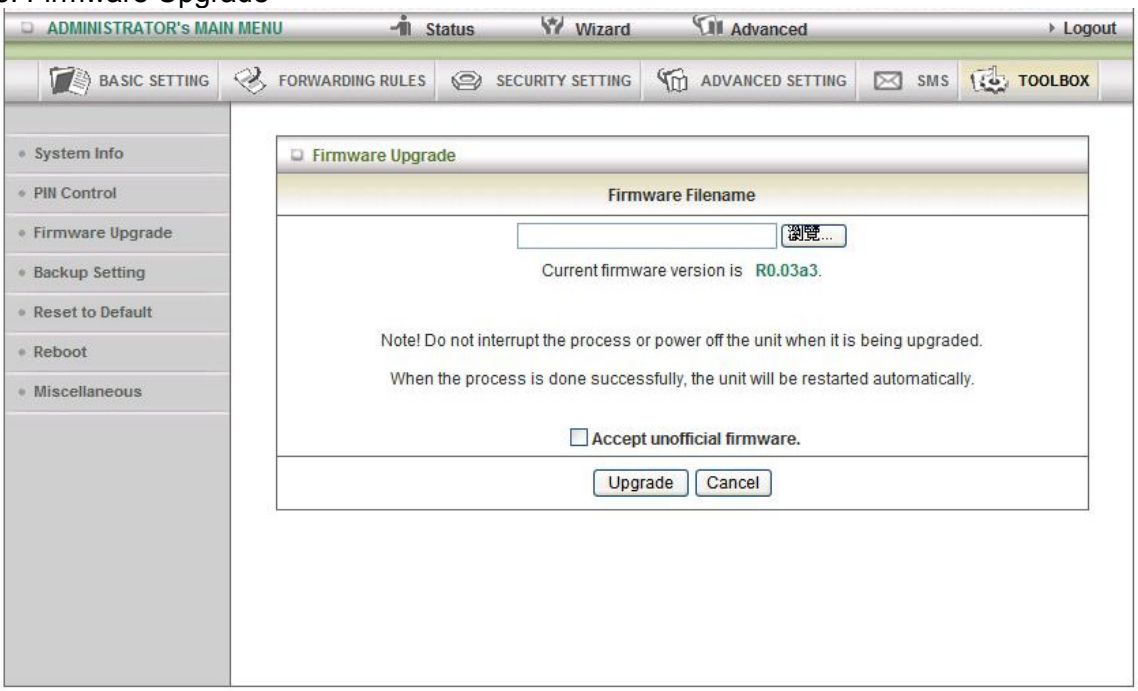
You can enable/disable the PIN Code control function, or change the PIN code.

1. PIN Code request function: Enable or Disable the PIN Code Request function.
2. Input SIM PIN code: Input the correct PIN code before the press the “save” button.
3. PIN Code charge function: change the PIN code on the SIM card.

Warring:

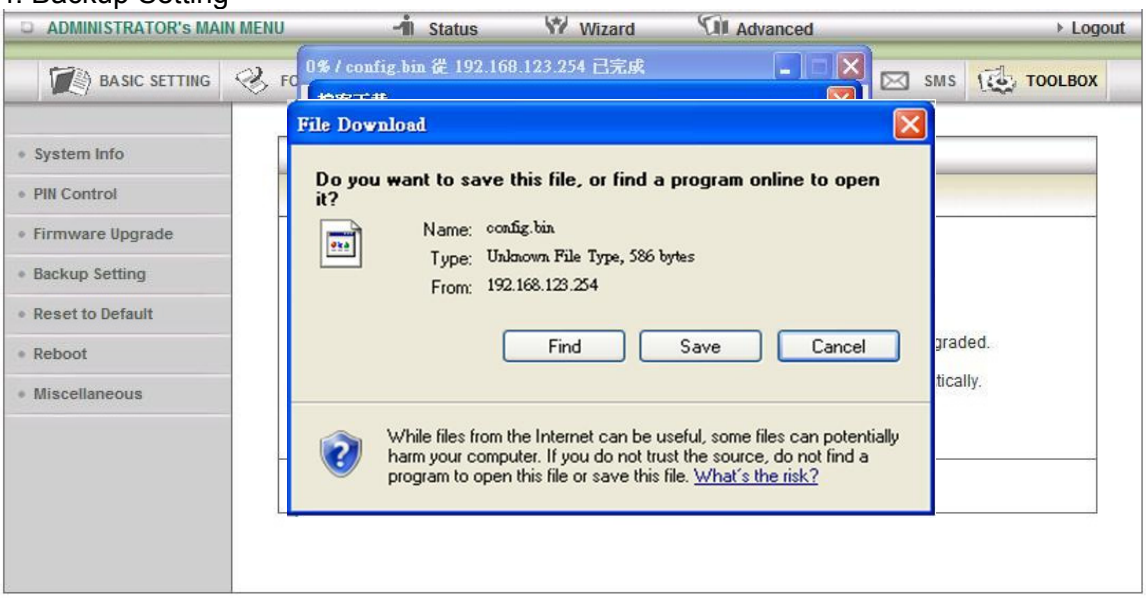
1. The SIM Card will be lock if retry more than 3 times.
2. The Page supports the Unlock SIM function too. You must get the PUK code from ISP first.

3. Firmware Upgrade



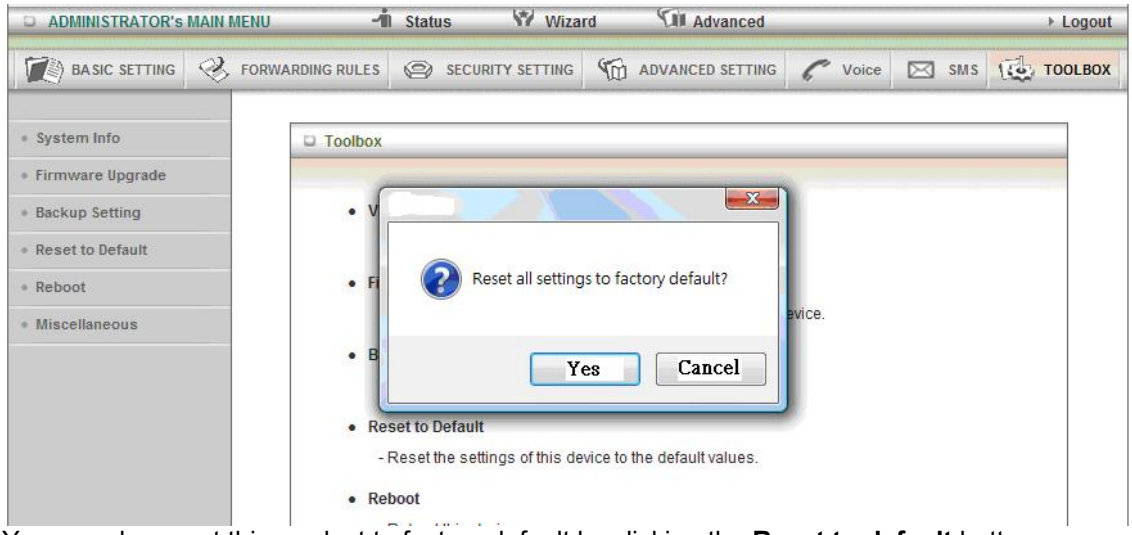
You can upgrade firmware by clicking “Upgrade” button.

4. Backup Setting



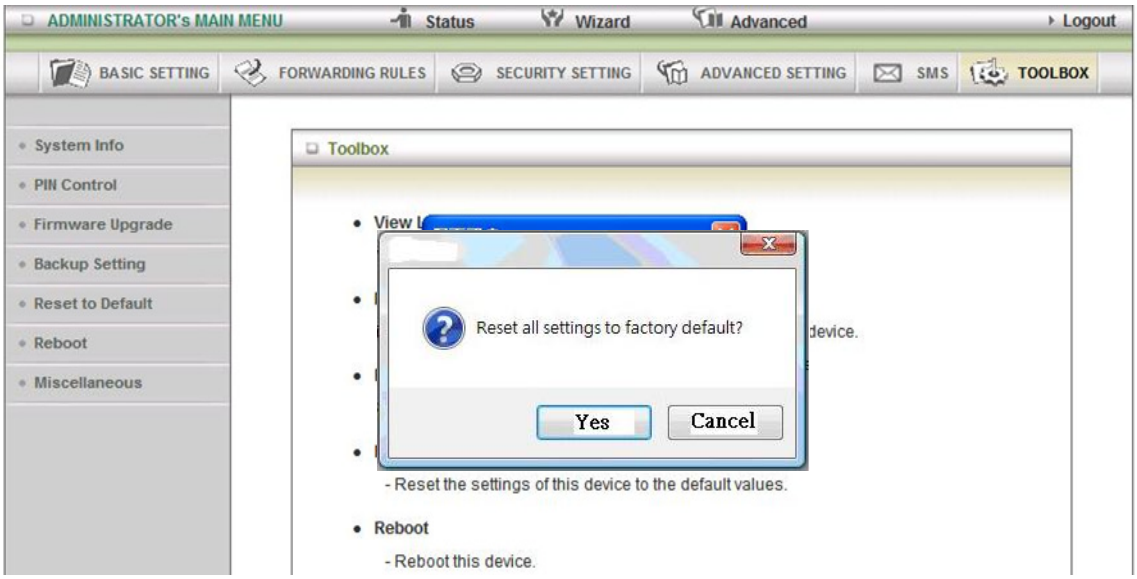
You can backup your settings by clicking the “**Backup Setting”** button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

5. Reset to Default



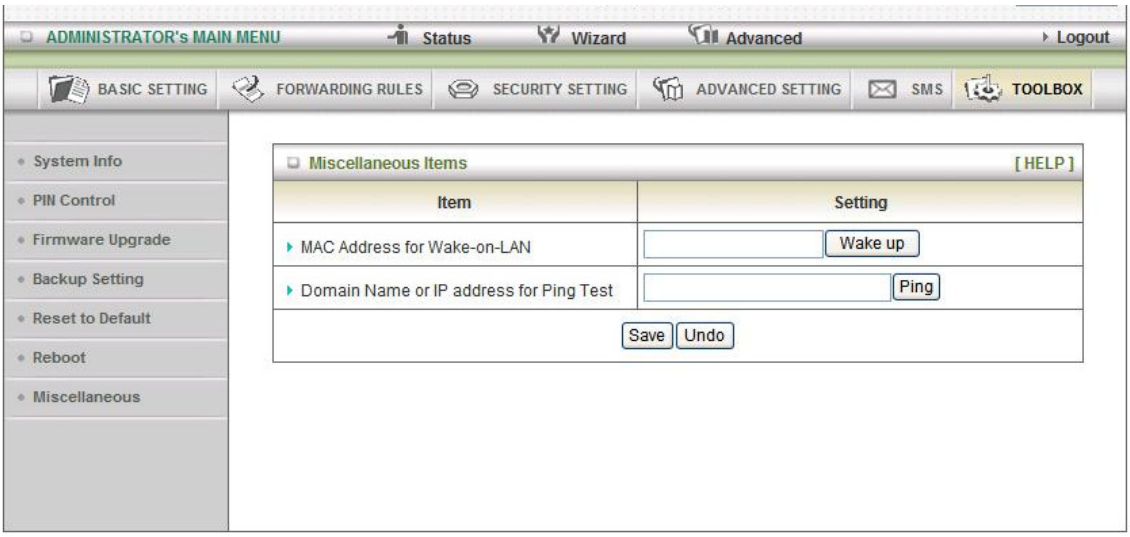
You can also reset this product to factory default by clicking the **Reset to default** button.

6. Reboot



You can also reboot this it by clicking the **Reboot** button.

7. Miscellaneous



Domain Name or IP address for Ping Test

Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

Chapter 4 Troubleshooting

This Chapter provides solutions to problems for the installation and operation of the 802.11n Wireless HSPA Router. You can refer to the following if you are having problems.

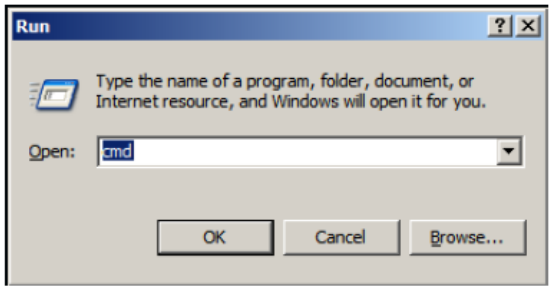
1 Why can't I configure the router even the cable is plugged and the LED is lit?

Do a **Ping test** to make sure that the 802.11n Wireless HSPA Router

Note: It is recommended that you use an Ethernet connection to configure it

Go to **Start > Run**.

1. Type **cmd**.



2. Press **OK.**
3. Type **ipconfig** to get the IP of default Router.
4. Type "**ping 192.168.123.254".** Assure that you ping the correct IP Address assigned to the WiFi HSPA IAD. It will show four replies if you ping correctly.

```
Pinging 192.168.123.254 with 32 bytes of data:

Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
```

Ensure that your Ethernet Adapter is working, and that all network drivers are installed properly. Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

1. Go to **Start > Right click on "My Computer" > Properties**.
2. **Select** the **Hardware Tab**.
3. Click **Device Manager**.
4. Double-click on "**Network Adapters"**.
5. Right-click on **Wireless Card bus Adapter** or **your specific network adapter**.
6. Select **Properties** to ensure that all drivers are installed properly.

7. Look under **Device Status** to see if the device is working properly.
8. Click "**OK"**.

2 What can I do if my Ethernet connection does not work properly?

A. Make sure the RJ45 cable connect with the router.

B. Ensure that the setting on your Network Interface Card adapter is "Enabled".

C. If settings are correct, ensure that you are not using a crossover Ethernet cable, not all Network Interface Cards are MDI/MDIX compatible, and use a patch cable is recommended.

D. If the connection still doesn't work properly, then you can reset it to default.

3 Problems with 3G connection?

A. What can I do if the 3G connection is failed by Auto detection?

Maybe the device can't recognize your ISP automatically. Please select "Manual" mode, and filling in dial-up settings manually.

B. What can I do if my country and ISP are not in the list?

Please choose "Others" item from the list, and filling in dial-up settings manually.

C. What can I do if my 3G connection is failed even the dongle is plugged?

Please check the following items:

I. Make sure you have inserted a validated SIM card in the 3G data card, and the subscription from ISP is still available

II. If you activate PIN code check feature in SIM card, making sure the PIN code you fill in dial-up page is correct

III. Checking with your ISP to see all dial-up settings are correct

IV. Make sure 3G signal from your ISP is available in your environment

D. What can I do if my router can't recognize my 3G data card even it is plugged?

There might be compatibility issue with some certain 3G cards. Please check the latest compatibility list to see if your 3G card is already supported.

E. What should I insert in APN, PIN Code, Account, Password, Primary DNS, and Secondary DNS?

The device will show this information after you choose country and Telcom. You can also check these values with your ISP.

F. Which 3G network should I select?

It depends on what service your ISP provide. Please check your ISP to know this information.

G. Why my 3G connection is keep dropping?

Please check 3G signal strength from your ISP in your environment is above middle

level.

4 Something wrong with the wireless connection?

A. Can't setup a wireless connection?

I. Ensure that the SSID and the encryption settings are exactly the same to the Clients.

II. Move the 802.11n Wireless HSPA Router and the wireless client into the same room, and then test the wireless connection.

III. Disable all security settings such as **WEP**, and **MAC Address Control**.

IV. Turn off the 802.11n Wireless HSPA Router and the client, then restart it and then turn on the client again.

V. Ensure that the LEDs are indicating normally. If no, make sure that the AC power and Ethernet cables are firmly connected.

VI. Ensure that the IP Address, subnet mask, Router and DNS settings are correctly entered for the network.

VII. If you are using other wireless device, home security systems or ceiling fans, lights in your home, your wireless connection may degrade dramatically. Keep your product away from electrical devices that generate RF noise such as microwaves, monitors, electric motors…

B. What can I do if my wireless client can not access the Internet?

I. Out of range: Put the router closer to your client.

II. Wrong SSID or Encryption Key: Check the SSID or Encryption setting.

III. Connect with wrong AP: Ensure that the client is connected with the correct Access Point.

i. **Right-click** on the **Local Area Connection icon** in the taskbar.

ii. Select **View Available Wireless Networks in Wireless Configure**. Ensure you have selected the correct available network.

iii. Reset the 802.11n Wireless HSPA Router to default setting

C. Why does my wireless connection keep dropping?

I. Antenna Orientation.

i. Try different antenna orientations for the 802.11n Wireless HSPA Router.

ii. Try to keep the antenna at least 6 inches away from the wall or other objects.

II. Try changing the channel on the 802.11n Wireless HSPA Router, and your Access Point and Wireless adapter to a different channel to avoid interference.

III. Keep your product away from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

5 What to do if I forgot my encryption key?

1. Go back to advanced setting to set up your Encryption key again.
2. Reset the 802.11n Wireless HSPA Router to default setting

6 How to reset to default?

1. Ensure the 802.11n Wireless HSPA Router is powered on
2. Find the **Reset** button on the right side
3. Press the **Reset** button for 8 seconds and then release.
4. After the 802.11n Wireless HSPA Router reboots, it has back to the factory **default** settings.

Appendix A Spec Summary Table

Device Interface		BDG561AM
Wireless WAN	Built-in HSUPA modem	1
Ethernet WAN/LAN	RJ-45 port, 10/100Mbps, 1xWAN / 4xLAN	1
Antenna	2 x PIFA internal antennas	2
WPS Button	For WPS connection	1
Reset Button	Reset router setting to factory default	1
LED Indication	Status / 3G signal Strength / 2.XG / 3.XG / SMS / WAN / LAN / WiFi	●
Power Button	Power ON/OFF button	1
Power Jack	Power Jack, DC 12V/1A	1
SIM Card Slot	For SIM card that users get from Telecom	1
Wireless LAN (WiFi)		
Standard	IEEE 802.11b/g/n (2x2) compliance	●
SSID	SSID broadcast or in stealth mode	●
Channel	Auto-selection, manually	●
Security	WEP, WPA-PSK, WPA2-PSK, WPA, WPA2	●
WPS	WPS (Wi-Fi Protected Setup)	●
Functionality		
Wireless WAN	PPP (for HSUPA)	●
Ethernet WAN	PPPoE, DHCP client, Static IP, PPTP, L2TP	●
WAN Connection	Auto-reconnect, dial-on-demand, manually	●
One-to-Many NAT	Virtual server, Special application, DMZ	●
SPI Firewall	IP/Service filter, URL blocking, MAC control	●
DoS Protection	DoS (Deny of Service) detection and protection	●
Management	SNMP, UPnP IGD, syslog	●
Administration	Web-based UI, remote login, backup/restore setting	●
Environment & Certification		
Package Information	Device dimension (mm)	●
	Package dimension (mm)	●
	Package weight (g)	●
Operation Temp.	Temp.: 0~40°C, Humidity 10%~90% non-condensing	●
Storage Temp.	Temp.: -10~70°C, Humidity: 0~95% non-condensing	●
EMI Certification	CE/FCC	●
RoHS	RoHS compliance	●

*Specifications are subject to change without prior notice.

Appendix B Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please refer to the GNU General Public License below to check the detailed terms of this license.

The following parts of this product are subject to the GNU GPL, and those software packages are copyright by their respective authors.

Linux-2.6.21 system kernel

busybox_1_00_rc2

bridge-utils 0.9.5

dhcpcd-1.3

ISC DHCP V2 P5

syslogd spread from busybox

wireless tools

ntpclient of NTP client implementation

GNU Wget

Availability of source code

Please visit our web site or contact us to obtain more information.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply

in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS